PCT/JP00/04488

JP00/4488

EKU

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

06.07.00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

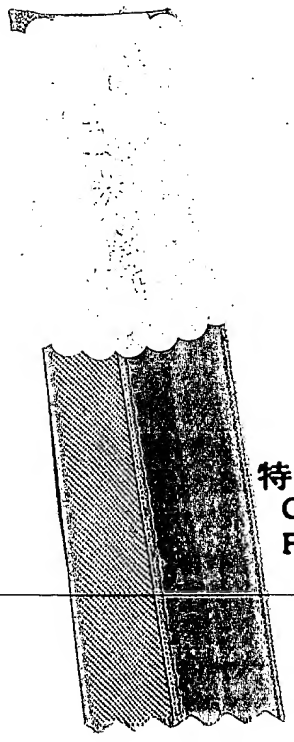
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　４月２１日

出願番号
Application Number: 特願２０００－１２６３０５

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)



２０００年　６月　９日

特許庁長官
Commissioner,
Patent Office

近藤隆彦

出証番号　出証特２０００－３０４３０２６

【書類名】　特許願
【整理番号】　0000438311
【提出日】　平成12年 4月21日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/16
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　野中　聡
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　江崎　正
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100094053
　【弁理士】
　【氏名又は名称】　佐藤　隆久
【先の出願に基づく優先権主張】
　【出願番号】　平成11年特許願第193562号
　【出願日】　平成11年 7月 7日
【手数料の表示】
　【予納台帳番号】　014890
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ提供システム、データ提供装置およびそれらの方法とデータ処理装置

【特許請求の範囲】

【請求項１】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項２】

前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項１に記載のデータ提供システム。

【請求項３】

前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項２に記載のデータ提供システム。

【請求項４】

前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよ

び前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項１に記載のデータ提供システム。

【請求項５】

前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項４に記載のデータ提供システム。

【請求項６】

前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項５に記載のデータ提供システム。

【請求項７】

前記データ提供装置は、

前記コンテンツデータを格納した第１のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第２のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項１に記載のデータ提供システム。

【請求項８】

前記データ提供装置は、前記第１のファイルおよび前記第２のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項７に記載のデータ提供システム。

【請求項９】

前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項８に記載のデータ提供システム。

【請求項１０】

前記データ提供装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項１に記載のデータ提供システム。

【請求項１１】

前記データ提供装置は、前記モジュールを記録した記録媒体を作成する

請求項１に記載のデータ提供システム。

【請求項１２】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項１に記載のデータ提供システム。

【請求項１３】

前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項１に記載のデータ提供システム。

【請求項１４】

前記データ処理装置は、前記モジュールに格納された公開鍵データを用いて、前記モジュールに格納された署名データの正当性を検証する

請求項９に記載のデータ提供システム。

【請求項１５】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項３に記載のデータ提供システム。

【請求項１６】

前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項１に記載のデータ提供システム。

【請求項１７】

データ提供装置から配給されたコンテンツデータを利用するデータ処理装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ処理装置。

【請求項１８】

データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項１９】

前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第２のモジュールを前記データ処理装置に配給する

請求項１８に記載のデータ提供システム。

【請求項２０】

前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記第１のモジュールを前記データ配給装置に提供し、

前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項１８に記載のデータ提供システム。

【請求項２１】

前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項２０に記載のデータ提供システム。

【請求項２２】

前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納し、前記配信用鍵データを用いて暗号化された第３のモジュールを格納した前記第１のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第３のモジュールを前記第２のモジュールに格納して前記データ処理装置に配給する

請求項２０に記載のデータ提供システム。

【請求項２３】

前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記第３のモジュールを格納した前記第１のモジュールを前記データ配給装置に提供する

請求項２２に記載のデータ提供システム。

【請求項２４】

前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記第３のモジュールを格納した前記第１のモジュールを前記データ配給装置に提供する

請求項２３に記載のデータ提供システム。

【請求項２５】

前記データ提供装置は、

前記コンテンツデータを格納した第１のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第２のファイルとを格納した前記第１のモジュールを前記データ配給装置に提供する

請求項１８に記載のデータ提供システム。

【請求項２６】

前記データ提供装置は、前記第１のファイルおよび前記第２のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記第１のモジュールを前記データ配給装置に提供する

請求項２５に記載のデータ提供システム。

【請求項２７】

前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格納した前記第１のモジュールを前記データ配給装置に提供する

請求項２５に記載のデータ提供システム。

【請求項２８】

前記データ配給装置は、前記価格データに対して自らの秘密鍵データを用いて署名データを作成し、当該署名データを前記第２のモジュールに格納して前記データ処理装置に配給する

請求項１９に記載のデータ提供システム。

【請求項２９】

前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記第２のモジュールを前記データ処理装置に提供する

請求項２８に記載のデータ提供システム。

【請求項３０】

前記データ配給装置は、前記第１のファイルおよび前記第２のファイルについての署名データを、前記データ提供装置の公開鍵データを用いて検証する

請求項２６に記載のデータ提供システム。

【請求項３１】

前記データ提供装置は、

前記第１のファイルと、第２のファイルとのリンク関係を示すリンクデータを格納した前記第１のモジュールを前記データ配給装置に提供する

請求項２５に記載のデータ提供システム。

【請求項３２】

前記データ配給装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記第２のモジュールを暗号化し、当該暗号化した第２のモジュールを前記データ処理装置に送信する

請求項１８に記載のデータ提供システム。

【請求項３３】

前記データ配給装置は、前記モジュールを記録した記録媒体を作成する

請求項１８に記載のデータ提供システム。

【請求項３４】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項１８に記載のデータ提供システム。

【請求項３５】

前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項１８に記載のデータ提供システム。

【請求項３６】

前記データ処理装置は、前記第２のモジュールに格納された公開鍵データを用いて、前記第２のモジュールに格納された署名データの正当性を検証する

請求項２９に記載のデータ提供システム。

【請求項３７】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項２１に記載のデータ提供システム。

【請求項３８】

前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項１８に記載のデータ提供システム。

【請求項３９】

データ提供装置と、少なくとも第１のデータ配給装置および第２のデータ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを前記複数のデータ配給装置に提供し、

前記第１のデータ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを前記データ処理装置に配給し、

前記第２のデータ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第３のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第２のモジュールおよび前記第

３のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項４０】

少なくとも第１のデータ提供装置および第２のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記第１のデータ提供装置は、第１のコンテンツ鍵データを用いて暗号化された第１のコンテンツデータと、暗号化された前記第１のコンテンツ鍵データと、前記第１のコンテンツデータの取り扱いを示す暗号化された第１の権利書データとを格納した第１のモジュールを前記データ配給装置に提供し、

前記第２のデータ提供装置は、第２のコンテンツ鍵データを用いて暗号化された第２のコンテンツデータと、暗号化された前記第２のコンテンツ鍵データと、前記第２のコンテンツデータの取り扱いを示す暗号化された第２の権利書データとを格納した第２のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化された前記第１のコンテンツデータ、前記第１のコンテンツ鍵データおよび前記第１の権利書データと、前記提供を受けた前記第２のモジュールに格納された前記暗号化された前記第２のコンテンツデータ、前記第２のコンテンツ鍵データおよび前記第２の権利書データとを格納した第３のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第３のモジュールに格納された前記第１のコンテンツ鍵データおよび前記第１の権利書データを復号し、当該復号した第１の権利書データに基づいて、前記第１のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第３のモジュールに格納された前記第２のコンテンツ鍵データおよび前記第２の権利書データを復号し、当該復号した第２の権利書データに基づいて、前記第２のコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項４１】

コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供装置。

【請求項４２】

前記権利書データを作成、当該作成した権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項４１に記載のデータ提供装置。

【請求項４３】

配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項４１に記載のデータ提供装置。

【請求項４４】

所定の権威機関が発行した前記配信用鍵データを用いて、前記コンテンツ鍵データＫｃおよび前記権利書データを暗号化する

請求項４３に記載のデータ提供装置。

【請求項４５】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項４１に記載のデータ提供装置。

【請求項４６】

自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項４５に記載のデータ提供装置。

【請求項４７】

前記公開鍵データの正当性を証明する公開鍵証明書データをを格納した前記モジュールを前記データ処理装置に配給する

請求項４６に記載のデータ提供装置。

【請求項４８】

前記コンテンツデータを格納した第１のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第２のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項４１に記載のデータ提供装置。

【請求項４９】

前記第１のファイルおよび前記第２のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項４８に記載のデータ提供装置。

【請求項５０】

前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項４９に記載のデータ提供装置。

【請求項５１】

前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項４１に記載のデータ提供装置。

【請求項５２】

前記モジュールを記録した記録媒体を作成する

請求項４１に記載のデータ提供装置。

【請求項５３】

前記モジュールをアプリケーション層で定義する

請求項４１に記載のデータ提供装置。

【請求項５４】

前記モジュールを前記データ処理装置に配給する配送プロトコルとして、前記アプリケーション層の下層のプレゼンテーション層およびトランスポート層を用いる

請求項５３に記載のデータ提供装置。

【請求項５５】

前記モジュールを前記データ処理装置に配給するための媒体に依存しない形式で前記モジュールを定義する

請求項４１に記載のデータ提供装置。

【請求項５６】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項５７】

前記データ提供装置から前記データ処理装置に、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項５６に記載のデータ提供方法。

【請求項５８】

データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項５９】

前記データ配給装置から前記データ処理装置に、前記コンテンツデータの価格を示す価格データを格納した前記第２のモジュールを配給する

請求項５８に記載のデータ提供方法。

【請求項６０】

データ提供装置と、少なくとも第１のデータ配給装置および第２のデータ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを提供し、

前記第１のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを配給し、

前記第２のデータ配給装置から前記データ処理装置に、前記提供を受けた前記

第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第３のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第２のモジュールおよび前記第３のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項６１】

少なくとも第１のデータ提供装置および第２のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記第１のデータ提供装置から前記データ配給装置に、第１のコンテンツ鍵データを用いて暗号化された第１のコンテンツデータと、暗号化された前記第１のコンテンツ鍵データと、前記第１のコンテンツデータの取り扱いを示す暗号化された第１の権利書データとを格納した第１のモジュールを提供し、

前記第２のデータ提供装置から前記データ配給装置に、第２のコンテンツ鍵データを用いて暗号化された第２のコンテンツデータと、暗号化された前記第２のコンテンツ鍵データと、前記第２のコンテンツデータの取り扱いを示す暗号化された第２の権利書データとを格納した第２のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化された前記第１のコンテンツデータ、前記第１のコンテンツ鍵データおよび前記第１の権利書データと、前記提供を受けた前記第２のモジュールに格納された前記暗号化された前記第２のコンテンツデータ、前記第２のコンテンツ鍵データおよび前記第２の権利書データとを格納した第３のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第３のモジュールに格納された前記第１のコンテンツ鍵データおよび前記第１の権利書データを復号し、当該復号した第１の権利書データに基づいて、前記第１のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第３のモジュールに格納された前記第２のコンテンツ鍵データおよび前記第２の権利書データを復号し、当該復号した第

２の権利書データに基づいて、前記第２のコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項６２】

コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供方法。

【請求項６３】

配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項６２に記載のデータ提供方法。

【請求項６４】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項６２に記載のデータ提供方法。

【請求項６５】

自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項６４に記載のデータ提供方法。

【請求項６６】

前記公開鍵データの正当性を証明する公開鍵証明書データをを格納した前記モジュールを前記データ処理装置に配給する

請求項６５に記載のデータ提供方法。

【請求項６７】

前記コンテンツデータを格納した第１のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第２のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項６２に記載のデータ提供方法。

【請求項６８】

前記第１のファイルおよび前記第２のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項６７に記載のデータ提供方法。

【請求項６９】

前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項６８に記載のデータ提供方法。

【請求項７０】

前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項６２に記載のデータ提供方法。

【請求項７１】

前記モジュールを記録した記録媒体を作成する

請求項６２に記載のデータ提供方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンテンツデータを提供するデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置に関する。

【０００２】

【従来の技術】

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生お

よび記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来のＥＭＤ(Electronic Music Distribution: 電子音楽配信）システムがある。

【０００３】

図１００は、従来のＥＭＤシステム７００の構成図である。

図１００に示すＥＭＤシステム７００では、コンテンツプロバイダ７０１ａ，７０１ｂが、サービスプロバイダ７１０に対し、コンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報７０５ａ，７０５ｂ，７０５ｃには、例えば、ＳＣＭＳ(Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ７１０の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【０００４】

サービスプロバイダ７１０は、受信したコンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとをセッション鍵データを用いて復号する。

そして、サービスプロバイダ７１０は、復号したあるいはオフラインで受け取ったコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに、著作権情報７０５ａ，７０５ｂ，７０５ｃを埋め込んで、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを生成する。このとき、サービスプロバイダ７１０は、例えば、著作権情報７０５ａ，７０５ｂ，７０５ｃのうち電子透かし情報をコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにＳＣＭＳ情報を埋め込む。

さらに、サービスプロバイダ７１０は、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、鍵データベース７０６から読み出したコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いてそれぞれ暗号化する。その後、サービスプロバイダ７１０は、暗号化されたコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを格納し

たセキュアコンテナ７２２を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置７０９に存在するＣＡ(Conditional Access)モジュール７１１に送信する。

【０００５】

ＣＡモジュール７１１は、セキュアコンテナ７２２をセッション鍵データを用いて復号する。また、ＣＡモジュール７１１は、電子決済やＣＡなどの課金機能を用いて、サービスプロバイダ７１０の鍵データベース７０６からコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置７０９において、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、それぞれコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号することが可能になる。

このとき、ＣＡモジュール７１１は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報７２１を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ７１０の権利処理モジュール７２０に送信する。

この場合に、ＣＡモジュール７１１は、サービスプロバイダ７１０が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティー確保とを行う。

【０００６】

サービスプロバイダ７１０は、ＣＡモジュール７１１から課金情報７２１を受信すると、サービスプロバイダ７１０とコンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃとの間で利益配分を行う。

このとき、サービスプロバイダ７１０から、コンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃへの利益配分は、例えば、ＪＡＳＲＡＣ(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会）を介して行われる。また、ＪＡＳＲＡＣによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【０００７】

また、端末装置７０９では、コンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号したコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、ＲＡＭ型の記録媒体７２３などに記録する際に、著作権情報７０５ａ，７０５ｂ，７０５ｃのＳＣＭＳビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃに埋め込まれたＳＣＭＳビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【０００８】

【発明が解決しようとする課題】

ところで、ＳＣＭＳは、ＣＤ(Compact Disc)からＤＡＴ(Digital Audio Tape)への録音を防止するために規定されたものであり、ＤＡＴとＤＡＴとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダを特定するに止まり、違法なコピーを技術的に阻止するものではない。

従って、上述した図１００に示すＥＭＤシステム７００では、コンテンツプロバイダの権利（利益）が十分に保護されないという問題がある。

【０００９】

また、上述したＥＭＤシステム７００では、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

【００１０】

また、上述したＥＭＤシステム７００では、ユーザの端末装置７０９からの課金情報７２１を、サービスプロバイダ７１０の権利処理モジュール７２０で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうかが懸念

される。

【００１１】

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置とを提供することを目的とする。

また、本発明は、コンテンプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置とを提供することを目的とする。

【００１２】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第１の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００１３】

本発明の第１の観点のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納したモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、

データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

【００１４】

また、本発明の第１の観点のデータ提供システムは、好ましくは、前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する。

【００１５】

また、本発明の第１の観点のデータ提供システムは、好ましくは、前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置をさらに有する。

【００１６】

また、本発明のデータ処理装置は、データ提供装置から配給されたコンテンツデータを利用するデータ処理装置であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００１７】

また、本発明の第２の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利

書データを格納した第２のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００１８】

本発明の第２の観点のデータ提供システムでは、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールが提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールが配給される。

次に、前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【００１９】

また、本発明の第２の観点のデータ提供システムは、好ましくは、前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第２のモジュールを前記データ処理装置に配給する。

【００２０】

また、本発明の第３の観点のデータ提供システムは、データ提供装置と、少なくとも第１のデータ配給装置および第２のデータ配給装置と、データ処理装置とを有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを前記複数のデータ配給装置に提供し、前記第１のデータ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納し

た第２のモジュールを前記データ処理装置に配給し、前記第２のデータ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第３のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第２のモジュールおよび前記第３のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００２１】

また、本発明の第４の観点のデータ提供システムは、少なくとも第１のデータ提供装置および第２のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムであって、前記第１のデータ提供装置は、第１のコンテンツ鍵データを用いて暗号化された第１のコンテンツデータと、暗号化された前記第１のコンテンツ鍵データと、前記第１のコンテンツデータの取り扱いを示す暗号化された第１の権利書データとを格納した第１のモジュールを前記データ配給装置に提供し、前記第２のデータ提供装置は、第２のコンテンツ鍵データを用いて暗号化された第２のコンテンツデータと、暗号化された前記第２のコンテンツ鍵データと、前記第２のコンテンツデータの取り扱いを示す暗号化された第２の権利書データとを格納した第２のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化された前記第１のコンテンツデータ、前記第１のコンテンツ鍵データおよび前記第１の権利書データと、前記提供を受けた前記第２のモジュールに格納された前記暗号化された前記第２のコンテンツデータ、前記第２のコンテンツ鍵データおよび前記第２の権利書データとを格納した第３のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第３のモジュールに格納された前記第１のコンテンツ鍵データおよび前記第１の権利書データを復号し、当該復号した第１の権利書データに基づいて、前記第１のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第３のモジュールに格納された前記第２のコンテンツ鍵データおよび前記第２の権利書データを復号し、当該復号した第２の権利書データに基づいて、前記第２のコンテンツデータの

取り扱いを決定する。

【００２２】

また、本発明のデータ提供装置は、コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する。

【００２３】

また、本発明の第１の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００２４】

また、本発明の第２の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００２５】

また、本発明の第３の観点のデータ提供方法は、データ提供装置と、少なくとも第１のデータ配給装置および第２のデータ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを提供し、前記第１のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを配給し、前記第２のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第３のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第２のモジュールおよび前記第３のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００２６】

また、本発明の第４の観点のデータ提供方法は、少なくとも第１のデータ提供装置および第２のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記第１のデータ提供装置から前記データ配給装置に、第１のコンテンツ鍵データを用いて暗号化された第１のコンテンツデータと、暗号化された前記第１のコンテンツ鍵データと、前記第１のコンテンツデータの取り扱いを示す暗号化された第１の権利書データとを格納した第１のモジュールを提供し、前記第２のデータ提供装置から前記データ配給装置に、第２のコンテンツ鍵データを用いて暗号化された第２のコンテンツデータと、暗号化された前記第２のコンテンツ鍵データと、前記第２のコンテンツデータの取り扱いを示す暗号化された第２の権利書データとを格納した第２のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第１のモジュールに格納された前記暗号化された前記第１のコンテンツデータ、前記第１

のコンテンツ鍵データおよび前記第１の権利書データと、前記提供を受けた前記第２のモジュールに格納された前記暗号化された前記第２のコンテンツデータ、前記第２のコンテンツ鍵データおよび前記第２の権利書データとを格納した第３のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第３のモジュールに格納された前記第１のコンテンツ鍵データおよび前記第１の権利書データを復号し、当該復号した第１の権利書データに基づいて、前記第１のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第３のモジュールに格納された前記第２のコンテンツ鍵データおよび前記第２の権利書データを復号し、当該復号した第２の権利書データに基づいて、前記第２のコンテンツデータの取り扱いを決定する。

【００２７】

【発明の実施の形態】

以下、本発明の実施形態に係わるＥＭＤ(Electronic Music Distribution: 電子音楽配信）システムについて説明する。

本実施形態において、ユーザに配信されるコンテンツ(Content）データとは、音楽データ、映像データおよびプログラムなど情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

【００２８】

第１実施形態

図１は、本実施形態のＥＭＤシステム１００の構成図である。

図１に示すように、ＥＭＤシステム１００は、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ（クリアリング・ハウス、以下、ＥＳＣとも記す）１０２およびユーザホームネットワーク１０３を有する。

ここで、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２およびＳＡＭ105_1～105_4が、それぞれ請求項１および請求項３などに係わるデータ提供装置、管理装置およびデータ処理装置に対応している。

先ず、ＥＭＤシステム１００の概要について説明する。

ＥＭＤシステム１００では、コンテンツプロバイダ１０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す

権利書(UCP:Usage Control Policy)データ１０６を、高い信頼性のある権威機関であるＥＭＤサービスセンタ１０２に送信する。権利書データ１０６は、ＥＭＤサービスセンタ１０２によって権威化（認証）される。

【００２９】

また、コンテンツプロバイダ１０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成すると共に、コンテンツ鍵データＫｃをＥＭＤサービスセンタ１０２から配給された対応する期間の配信用鍵データKD_1～$KD5_6$で暗号化する。そして、コンテンツプロバイダ１０１は、暗号化されたコンテンツ鍵データＫｃおよびコンテンツファイルＣＦと自らの署名データとを格納（カプセル化）したセキュアコンテナ（本発明のモジュール）１０４を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク１０３に配給する。

このように、本実施形態では、デジタルのコンテンツデータＣをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路（配送チャンネル）を介して提供されても、コンテンツデータＣ（商品）を販売するときの最も基本となる商品カプセルである。具体的には、セキュアンテナは、課金を行うための暗号情報や、コンテンツデータＣの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

【００３０】

ユーザホームネットワーク１０３は、例えば、ネットワーク機器160_1およびＡＶ機器160_2～160_4を有する。

ネットワーク機器160_1は、ＳＡＭ(Secure Application Module) 105_1を内蔵している。

ＡＶ機器160_2～160_4は、それぞれＳＡＭ105_2～105_4を内蔵している。ＳＡＭ105_1～105_4相互間は、例えば、ＩＥＥＥ(Institute of

Electrical and Electronics Engineers) １３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

【００３１】

ＳＡＭ１０５$_1$～１０５$_4$は、ネットワーク機器１６０$_1$がコンテンツプロバイダ１０１からネットワークなどを介してオンラインで受信したセキュアコンテナ１０４、および／または、コンテンツプロバイダ１０１からＡＶ機器１６０$_2$～１６０$_4$に記録媒体を介してオフラインで供給されたセキュアコンテナ１０４を対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて復号した後に、署名データの検証を行う。

ＳＡＭ１０５$_1$～１０５$_4$に供給されたセキュアコンテナ１０４は、ネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

ＳＡＭ１０５$_1$～１０５$_4$は、上述したセキュアコンテナ１０４の購入・利用の履歴を利用履歴(Usage Log) データ１０８として記録する。

利用履歴データ１０８は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じて、ユーザホームネットワーク１０３からＥＭＤサービスセンタ１０２に送信される。

【００３２】

ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づいて、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが決済機関９１に支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１に支払われる。

また、ＥＭＤサービスセンタ１０２は、一定期間毎に、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【００３３】

本実施形態では、ＥＭＤサービスセンタ１０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、ＥＭＤサービスセンタ１０２は、中立の立場にある最高の権威機関であるルート認証局９２に対しての（ルート認証局９２の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_4$において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ１０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の権利書データ１０６を登録して権威化することも、ＥＭＤサービスセンタ１０２の認証機能の一つである。

また、ＥＭＤサービスセンタ１０２は、例えば、配信用鍵データＫＤ$_1$～ＫＤ$_6$などの鍵データの管理を行なう鍵データ管理機能を有する。

また、ＥＭＤサービスセンタ１０２は、権威化した権利書データ１０６に記述された標準小売価格ＳＲＰ(Suggested Retailer' Price)とＳＡＭ１０５$_1$～ＳＡＭ１０５$_4$から入力した利用履歴データ１０８とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ１０１に分配する権利処理（利益分配）機能を有する。

【００３４】

以下、コンテンツプロバイダ１０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ１０１〕

図２は、コンテンツプロバイダ１０１の機能ブロック図であり、ユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$との間で送受信されるデータに関連するデータの流れが示されている。

また、図３には、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間で送受信されるデータに関連するデータの流れが示されている。

なお、図３以降の図面では、署名データ処理部、および、セッション鍵データK_{SES}を用いた暗号化・復号部に入出力するデータの流れは省略している。

【００３５】

図２および図３に示すように、コンテンツプロバイダ１０１は、コンテンツマスタソースサーバ１１１、電子透かし情報付加部１１２、圧縮部１１３、暗号化

部１１４、乱数発生部１１５、暗号化部１１６、署名処理部１１７、セキュアコンテナ作成部１１８、セキュアコンテナデータベース１１８ａ、記憶部１１９、相互認証部１２０、暗号化・復号部１２１、権利書データ作成部１２２、ＳＡＭ管理部１２４およびＥＭＤサービスセンタ管理部１２５を有する。

コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでＥＭＤサービスセンタ１０２に登録し、自らの識別子（識別番号）ＣＰ＿ＩＤを得る。また、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から、ＥＭＤサービスセンタ１０２の公開鍵データと、ルート認証局９２の公開鍵データとを受ける。

以下、図２および図３に示すコンテンツプロバイダ１０１の各機能ブロックについて説明する。

【００３６】

コンテンツマスタソースサーバ１１１は、ユーザホームネットワーク１０３に提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータＳ１１１を電子透かし情報付加部１１２に出力する。

【００３７】

電子透かし情報付加部１１２は、コンテンツデータＳ１１１に対して、ソース電子透かし情報(Source Watermark)Ｗｓ、コピー管理用電子透かし情報(Copy Control Watermark)Ｗｃおよびユーザ電子透かし情報(User Watermark)Ｗｕなどを埋め込んでコンテンツデータＳ１１２を生成し、コンテンツデータＳ１１２を圧縮部１１３に出力する。

【００３８】

ソース電子透かし情報Ｗｓは、コンテンツデータの著作権者名、ＩＳＲＣコード、オーサリング日付、オーサリング機器ＩＤ(Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Ｗｃは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Ｗｕには、例えば、セキュアコンテナ１０４の配給元および配給先を特定するためのコンテンツプロバイダ１０１の識

別子ＣＰ＿ＩＤおよびユーザホームネットワーク１０３のＳＡＭ１０$5_1$～１０$5_4$の識別子ＳＡＭ＿ＩＤ$_1$～ＳＡＭ＿ＩＤ$_4$が含まれる。

また、電子透かし情報付加部１１２は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のＩＤを電子透かし情報としてコンテンツデータＳ１１１に埋め込む。

本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、ＥＭＤサービスセンタ１０２において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク１０３内のネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク１０３では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【００３９】

圧縮部１１３は、コンテンツデータＳ１１２を、例えば、ＡＴＲＡＣ３(Adaptive Transform Acoustic Coding 3)（商標）などの音声圧縮方式で圧縮し、圧縮したコンテンツデータＳ１１３を暗号化部１１４に出力する。

【００４０】

暗号化部１１４は、コンテンツ鍵データＫｃを共通鍵として用い、ＤＥＳ(Data Encryption Standard)やＴｒｉｐｌｅ　ＤＥＳなどの共通鍵暗号化方式で、コンテンツデータＳ１１３を暗号化してコンテンツデータＣを生成し、これをセキュアコンテナ作成部１１８に出力する。

また、暗号化部１１４は、コンテンツ鍵データＫｃを共通鍵として用い、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよびメタデータＭｅｔａを暗号化した後に、セキュアコンテナ作成部１１７に出力する。

【００４１】

ＤＥＳは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして

処理する暗号化方式である。ＤＥＳの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。ＤＥＳの全てのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【００４２】

先ず、平文の６４ビットは、上位３２ビットのH_0と下位３２ビットのL_0とに分割される。鍵処理部から供給された４８ビットの拡大鍵データK_1および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を撹拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力との排他的論理和が算出され、その結果はL_1とされる。また、L_0は、H_1とされる。

そして、上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【００４３】

乱数発生部１１５は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データＫｃとして暗号化部１１４および暗号化部１１６に出力する。

なお、コンテンツ鍵データＫｃは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データＫｃは、例えば、所定時間毎に更新される。

【００４４】

暗号化部１１６は、後述するようにしてＥＭＤサービスセンタ１０２から受信されて記憶部１１９に記憶された配信用鍵データKD_1～KD_6のうち対応する期間の配信用鍵データKD_1～KD_6を入力し、当該配信用鍵データを共通鍵として用いたＤＥＳなどの共通暗号化方式によって図４（Ｂ）に示すコンテンツ鍵データＫｃ、権利書データ１０６、ＳＡＭプログラム・ダウンロード・コンテナ

SDC_1～SDC_3および署名・証明書モジュールMod_1を暗号化した後に、セキュアコンテナ作成部１１７に出力する。

署名・証明書モジュールMod_1には、図４（Ｂ）に示すように、署名データ$SIG_{2,CP}$～$SIG_{4,CP}$、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}および当該公開鍵証明書CER_{CP}に対してのＥＭＤサービスセンタ１０２の署名データ$SIG_{1,ESC}$が格納されている。

また、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3は、ＳＡＭ105_1～105_4内でプログラムのダウンロードを行なう際に用いられるダウンロード・ドライバと、権利書データ（ＵＣＰ）Ｕ１０６のシンタックス（文法）を示すＵＣＰ－Ｌ(Label)．Ｒ(Reader)と、ＳＡＭ105_1～105_4に内蔵された記憶部（フラッシュ－ＲＯＭ）の書き換えおよび消去をブロック単位でロック状態／非ロック状態にするためのロック鍵データとを格納している。

【００４５】

なお、記憶部１１９は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データKD_1～KD_6を記憶するデータベースおよびキーファイルＫＦを記憶するデータベースなどの種々のデータベースを備えている。

【００４６】

署名処理部１１７は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いて、その署名データＳＩＧを作成する。

【００４７】

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【００４８】

セキュアコンテナ作成部１１８は、図４（Ａ）に示すように、ヘッダデータと

、暗号化部１１４から入力したそれぞれコンテンツ鍵データＫｃで暗号化されたコンテンツデータＣ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよびメタデータＭｅｔａとを格納したコンテンツファイルＣＦを生成する。

ここで、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔは、ユーザホームネットワーク１０３のネットワーク機器160_1およびＡＶ機器160_2～160_4において、コンテンツファイルＣＦを伸長する際に用いられるソフトウェアであり、例えば、ＡＴＲＡＣ３方式の伸長用ソフトウェアである。

【００４９】

また、セキュアコンテナ作成部１１８は、図４（Ｂ）に示すように、暗号化部１１６から入力した対応する期間の配信用鍵データKD_1～KD_6で暗号化されたコンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3および署名・証明書モジュールMod_1を格納したキーファイルＫＦを生成する。

そして、セキュアコンテナ作成部１１８は、図４（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびキーファイルＫＦと、図４（Ｃ）に示すコンテンツプロバイダ１０１の公開鍵データK_{CP}および署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を生成し、これをセキュアコンテナデータバース１１８ａに格納した後に、ユーザからの要求に応じてＳＡＭ管理部１２４に出力する。

このように、本実施形態では、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をセキュアコンテナ１０４に格納してユーザホームネットワーク１０３に送信するイン・バンド(In-band) 方式を採用している。従って、ユーザホームネットワーク１０３は、公開鍵証明書CER_{CP}を得るための通信をＥＭＤサービスセンタ１０２との間で行う必要がない。

なお、本発明では、公開鍵証明書CER_{CP}をセキュアコンテナ１０４に格納しないで、ユーザホームネットワーク１０３がＥＭＤサービスセンタ１０２から公開鍵証明書CER_{CP}を得るアウト・オブ・バンド(Out-Of-band) 方式を採用してもよい。

【００５０】

相互認証部１２０は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１

０２およびユーザホームネットワーク１０３との間でオンラインでデータを送受信する際に、それぞれＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【００５１】

暗号化・復号部１２１は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３にオンラインで送信するデータを、セッション鍵データK_{SES}を用いて暗号化する。

また、暗号化・復号部１２１は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３からオンラインで受信したデータを、セッション鍵データK_{SES}を用いて復号する。

【００５２】

権利書データ作成部１２２は、権利書データ１０６を作成し、これを暗号化部１１６に出力する。

権利書データ１０６は、コンテンツデータＣの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ１０１の運用者が希望する標準小売価格ＳＲＰ(Suggested Retailer' Price) やコンテンツデータＣの複製ルールなどが記述されている。

【００５３】

ＳＡＭ管理部１２４は、セキュアコンテナ１０４を、オフラインおよび／またはオンラインでユーザホームネットワーク１０３に供給する。

ＳＡＭ管理部１２４は、ＣＤ－ＲＯＭやＤＶＤ(Digital Versatile Disc)などのＲＯＭ型の記録媒体（メディア）を用いてセキュアコンテナ１０４をオフラインでユーザホームネットワーク１０３に配給する場合には、配信用鍵データKD_1～KD_6などを用いてセキュアコンテナ１０４を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク１０３にオフラインで供給される。

【００５４】

本実施形態では、セキュアコンテナ（商品カプセル）１０４は、図５に示すよ

うに、ＯＳＩレイヤ層におけるアプリケーション層で定義される。また、プレゼンテーション層やトランスポート層に相当するカプセルは、セキュアコンテナを配送するための配送プロトコルとして、セキュアコンテナ１０４とは別に定義される。従って、セキュアコンテナ１０４を配送プロトコルに依存しないで定義できる。すなわち、セキュアコンテナ１０４を、例えばオンラインおよびオフラインの何れの形態でユーザホームネットワーク１０３に供給する場合でも、共通のルールに従って定義および生成できる。

例えば、セキュアコンテナ１０４をネットワークを使って供給する場合には、セキュアコンテナ１０４をコンテンツプロバイダ１０１の領域で定義し、プレゼンテーション層およびトランスポート層をセキュアコンテナ１０４をユーザホームネットワーク１０３まで搬送するための搬送ツールと考える。

また、オフラインの場合に、ＲＯＭ型の記録媒体を、セキュアコンテナ１０４をユーザホームネットワーク１０３に搬送する搬送キャリアとして考える。

【００５５】

図６は、ＲＯＭ型の記録媒体１３０を説明するための図である。

図６に示すように、ＲＯＭ型の記録媒体１３０は、ＲＯＭ領域１３１、ＲＡＭ領域１３２およびメディアＳＡＭ１３３を有する。

ＲＯＭ領域１３１には、図４（Ａ）に示したコンテンツファイルＣＦが記憶されている。

また、ＲＡＭ領域１３２には、図４（Ｂ）、（Ｃ）に示したキーファイルＫＦおよび公開鍵証明書データ$ＣＥＲ_{CP}$と機器の種類に応じて固有の値を持つ記録用鍵データ$Ｋ_{STR}$とを引数としてＭＡＣ(Message Authentication Code) 関数を用いて生成したと署名データと、当該キーファイルＫＦおよび公開鍵証明書データ$ＣＥＲ_{CP}$とを記録媒体に固有の値を持つメディア鍵データ$Ｋ_{MED}$を用いて暗号化したデータとが記憶される。

また、ＲＡＭ領域１３２には、例えば、不正行為などで無効となったコンテンツプロバイダ１０１および$ＳＡＭ１０５_{1}$～１０５_{5}を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

また、また、ＲＡＭ領域１３２には、後述するようにユーザホームネットワー

ク１０３のＳＡＭ１０５$_1$～１０５$_4$においてコンテンツデータＣの購入・利用形態が決定されたときに生成される利用制御状態（ＵＣＳ）データ１６６などが記憶される。これにより、利用制御状態データ１６６がＲＡＭ領域１３２に記憶されることで、購入・利用形態が決定したＲＯＭ型の記録媒体１３０となる。

メディアＳＡＭ１３３には、例えば、ＲＯＭ型の記録媒体１３０の識別子であるメディアＩＤと、メディア鍵データK_{MED}とが記憶されている。

メディアＳＡＭ１３３は、例えば、相互認証機能を有している。

【００５６】

また、ＳＡＭ管理部１２４は、セキュアコンテナ１０４を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク１０３に配信する場合には、暗号化・復号部１２１においてセッション鍵データK_{SES}を用いてセキュアコンテナ１０４を暗号化した後に、ネットワークを介してユーザホームネットワーク１０３に配信する。

本実施形態では、ＳＡＭ管理部、ＥＭＤサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【００５７】

ここで、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給は、上述したように記録媒体１３０を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ１０６が格納された共通の形式のセキュアコンテナ１０４を用いる。従って、ユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ１０６に基づいた権利処理を行なうことができる。

【００５８】

また、上述したように、本実施形態では、セキュアコンテナ１０４内に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、当該暗号化を解くためのコンテンツ鍵データＫｃとを同封するイン・バンド(In-Band) 方式を採用し

ている。イン・バンド方式では、ユーザホームネットワーク１０３の機器で、コンテンツデータＣを再生しようとするときに、コンテンツ鍵データＫｃを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データＫｃは配信用鍵データKD_1～KD_6で暗号化されているが、配信用鍵データKD_1～KD_6は、ＥＭＤサービスセンタ１０２で管理されており、ユーザホームネットワーク１０３のＳＡＭ105_1～105_5に事前に（ＳＡＭ105_1～105_4がＥＭＤサービスセンタ１０２に初回にアクセスする際に）配信されているので、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２との間をオンラインで接続することなく、オフラインで、コンテンツデータＣの利用が可能になる。

なお、本発明は、コンテンツデータＣとコンテンツ鍵データＫｃとを別々に、ユーザホームネットワーク１０３に供給するアウト・オブ・バンド(Out-Of-Band）方式を採用できる柔軟性を有している。

【００５９】

ＥＭＤサービスセンタ管理部１２５は、ＥＭＤサービスセンタ１０２から６カ月分の配信用鍵データKD_1～KD_6およびそれぞれに対応した署名データ$SIG_{KD1,ESC}$～$SIG_{KD6,ESC}$と、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を含む公開鍵証明書CER_{CP}およびその署名データ$SIG_{1,ESC}$と、決済レポートデータ１０７とを受信すると、これらを暗号化・復号部１２１においてセッション鍵データK_{SES}を用いて復号した後に、記憶部１１９に記憶する。

決済レポートデータ１０７は、例えば、ＥＭＤサービスセンタ１０２が図１に示す決済機関９１に対して行なったコンテンツプロバイダ１０１に関する決済の内容が記述されている。

【００６０】

また、ＥＭＤサービスセンタ管理部１２５は、提供するコンテンツデータＣのグローバルユニーク(Global Unique) な識別子Ｃｏｎｔｅｎｔ＿ＩＤ、公開鍵データ$K_{CP,P}$およびそれらの署名データ$SIG_{9,CP}$を、ＥＭＤサービスセンタ１０２に送信し、ＥＭＤサービスセンタ１０２から、公開鍵データ$K_{CP,P}$の公開鍵証明書データCER_{CP}を入力する。

また、ＥＭＤサービスセンタ管理部１２５は、権利書データ１０６をＥＭＤサービスセンタ１０２に登録する際に、図７（Ａ）に示すように、提供するコンテンツデータＣのグルーバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤ、コンテンツ鍵データＫｃおよび権利書データ１０６を格納したモジュールMod_3と、その署名データ$SIG_{5,CP}$とを格納した権利書登録要求用モジュールMod_2を作成し、これを暗号化・復号部１２１においてセッション鍵データK_{SES}を用いて暗号化した後に、ネットワークを介してＥＭＤサービスセンタ１０２に送信する。

ＥＭＤサービスセンタ管理部１２５としては、前述したように、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【００６１】

以下、図２および図３を参照しながら、コンテンツプロバイダ１０１における処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ１０１の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ１０２に登録処理を行い、グローバルユニークな識別子ＣＰ＿ＩＤを得ている。識別子ＣＰ＿ＩＤは、記憶部１１９に記憶される。

【００６２】

以下、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２に、自らの秘密鍵データ$K_{CP,S}$に対応する公開鍵データ$K_{CP,S}$の正当性を証明する公開鍵証明書データCER_{CP}を要求する場合の処理を図３および図８を参照しながら説明する。

図８は、当該処理のフローチャートである。

ステップＳＡ１：コンテンツプロバイダ１０１は、例えば真性乱数発生器から構成される乱数発生部１１５を用いて乱数を発生して秘密鍵データ$K_{CP,S}$を生成する。

ステップＳＡ２：コンテンツプロバイダ１０１は、秘密鍵データ$K_{CP,S}$に対応する公開鍵データ$K_{CP,P}$を作成して記憶部１１９に記憶する。

ステップＳＡ３：コンテンツプロバイダ１０１のＥＭＤサービスセンタ管理部１２５は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよび公開鍵データ$K_{CP,P}$を記憶部１１９から読み出す。

そして、ＥＭＤサービスセンタ管理部１２５は、識別子ＣＰ＿ＩＤおよび公開鍵データ$K_{CP,P}$を含む公開鍵証明書データ発行要求をＥＭＤサービスセンタ１０２に送信する。

ステップＳＡ４：ＥＭＤサービスセンタ管理部１２５は、当該発行要求に応じて、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$をＥＭＤサービスセンタ１０２から入力して記憶部１１９に書き込む。

【００６３】

以下、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２から配信用鍵データを受信する処理を図３を参照しながら説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から既に公開鍵証明書データCER_{CP}を得ている必要がある。

ＥＭＤサービスセンタ管理部１２５が、ＥＭＤサービスセンタ１０２から６カ月分の配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD6,ESC}$を入力し、これを記憶部１１９内の所定のデータベースに記憶する。

そして、署名処理部１１７において、記憶部１１９に記憶された署名データ$SIG_{KD1,ESC}$～$SIG_{KD6,ESC}$の正当性が確認された後に、記憶部１１９に記憶されている配信用鍵データKD_1～KD_6が有効なものとして扱われる。

【００６４】

以下、コンテンツプロバイダ１０１がユーザホームネットワーク１０３のＳＡＭ105_1にセキュアコンテナ１０４を送信する場合の処理を図２および図９を参照しながら説明する。

図９は、当該処理のフローチャートである。

なお、以下の例では、コンテンツプロバイダ１０１からＳＡＭ105_1にセキュアコンテナ１０４を送信する場合を例示するが、セキュアコンテナ１０４をＳ

ＡＭ１０５$_2$～１０５$_4$に送信する場合も、ＳＡＭ１０５$_1$を介してＳＡＭ１０５$_2$～１０５$_4$に送信される点を除いて同じである。

【００６５】

ステップＳＢ１：コンテンツデータＳ１１１がコンテンツマスタソースサーバ１１１から読み出されて電子透かし情報付加部１１２に出力される。

電子透かし情報付加部１１２は、コンテンツデータＳ１１１に電子透かし情報を埋め込んでコンテンツデータＳ１１２を生成し、これを圧縮部１１３に出力する。

ステップＳＢ２：圧縮部１１３は、コンテンツデータＳ１１２を、例えばＡＴＲＡＣ３方式で圧縮してコンテンツデータＳ１１３を作成し、これを暗号化部１１４に出力する。

【００６６】

ステップＳＢ３：乱数発生部１１５は、乱数を発生してコンテンツ鍵データＫｃを生成し、これを暗号化部１１４に出力する。

【００６７】

ステップＳＢ４：暗号化部１１４は、コンテンツデータＳ１１３と、記憶部１１９から読み出されたメタデータＭｅｔａおよびＡ／Ｖ伸長用ソフトウェアＳｏｆｔとを、コンテンツ鍵データＫｃを用いて暗号化してセキュアコンテナ作成部１１８に出力する。この場合に、メタデータＭｅｔａは暗号化しなくてもよい。

そして、セキュアコンテナ作成部１１８は、図４（Ａ）に示すコンテンツファイルＣＦを作成する。また、署名処理部１１７において、コンテンツファイルＣＦのハッシュ値がとられ、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{6,CP}$が生成される。

【００６８】

ステップＳＢ５：署名処理部１１７は、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６のそれぞれに対してハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて、それぞれのデータの作成者（提供者）の正当性を示す署名データ$SIG_{2,CP}$，$SIG_{3,CP}$，$SIG_{4,CP}$を作成する。

また、暗号化部１１６は、図４（Ｂ）に示すコンテンツ鍵データＫｃ、権利書

データ１０６、ＳＡＭプログラム・ダウンロード・コンテナSD_1～SD_3および署名・証明書モジュールMod_1を、対応する期間の配信用鍵データKD_1～KD_3で暗号化してセキュアコンテナ作成部１１８に出力する。

そして、セキュアコンテナ作成部１１８は、図４（Ｂ）に示すキーファイルＫＦを作成する。

また、署名処理部１１７は、キーファイルＫＦのハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて、署名データ$SIG_{7,CP}$を作成する。

【００６９】

ステップＳＢ６：セキュアコンテナ作成部１１８は、図４（Ａ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、図４（Ｂ）に示すキーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、図４（Ｃ）に示す公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を作成し、これを、セキュアコンテナデータベース１１８ａに記憶する。

ステップＳＢ７：セキュアコンテナ作成部１１８は、例えばユーザからの要求（リクエスト）に応じてユーザホームネットワーク１０３に提供しようとするセキュアコンテナ１０４をセキュアコンテナデータベース１１８ａから読み出して、相互認証部１２０と$SAM105_1$との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部１２１において暗号化した後に、ＳＡＭ管理部１２４を介してユーザホームネットワーク１０３の$SAM105_1$に送信する。

【００７０】

以下、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２に権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化することを要求する場合の処理を図３を参照して説明する。

権利書データ１０６およびコンテンツ鍵データＫｃの権威化要求処理は、個々のコンテンツデータＣ毎に行われる。

【００７１】

この場合には、署名処理部１１７において、記憶部１１９から読み出したコン

テンツデータＣのグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤ、コンテンツ鍵データＫｃおよび権利書データ作成部１２２から入力した権利書データ１０６からなるモジュールMod_3のハッシュ値が求められ、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{5,CP}$が生成される。

そして、図７（Ａ）に示す権利登録要求用モジュールMod_2を、相互認証部１２０とＥＭＤサービスセンタ１０２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部１２１において暗号化した後に、ＥＭＤサービスセンタ管理部１２５からＥＭＤサービスセンタ１０２に送信する。

【００７２】

本実施形態では、ＥＭＤサービスセンタ１０２において権利書データ１０６およびコンテンツ鍵データＫｃを権威化した後に、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ１０１において配信用鍵データKD_1～KD_6を用いて暗号化を行ってキーファイルＫＦを作成する場合を例示する。

但し、本発明は、例えば、ＥＭＤサービスセンタ１０２において権利書データ１０６およびコンテンツ鍵データＫｃを権威化した後に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に、配信用鍵データKD_1～KD_6を用いて暗号化した図７（Ｂ）に示す権威化証明書モジュールMod_{2a}を送信してもよい。

権威化証明書モジュールMod_{2a}は、コンテンツデータＣのグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤ、コンテンツ鍵データＫｃおよび権利書データ作成部１２２から入力した権利書データ１０６を格納したモジュールMod_{3a}と、秘密鍵データ$K_{ESC,S}$を用いたモジュールMod_{3a}の署名データ$SIG_{5a,ESC}$とを格納している。

この場合には、コンテンツプロバイダ１０１は、例えば、セキュアコンテナ１０４内に、権威化証明書モジュールMod_{2a}を格納してＳＡＭ105_1～105_4に配給する。

なお、ＥＭＤサービスセンタ１０２は、それぞれ異なる月に対応する配信用鍵

データKD_1～KD_6を用いて暗号化した６カ月分の権威化証明書モジュールMod_{2a}を生成し、これらをまとめてコンテンツプロバイダ１０１に送信してもよい。

【００７３】

〔ＥＭＤサービスセンタ１０２〕

ＥＭＤサービスセンタ１０２は、認証（ＣＡ:Certificate Authority）機能、鍵管理(Key Management)機能および権利処理(Rights Clearing)（利益分配）機能を有する。

図１０は、ＥＭＤサービスセンタ１０２の機能の構成図である。

図１０に示すように、ＥＭＤサービスセンタ１０２は、鍵サーバ１４１、鍵データベース１４１ａ、決算処理部１４２、署名処理部１４３、決算機関管理部１４４、証明書・権利書管理部１４５、ＣＥＲデータベース１４５ａ、コンテンツプロバイダ管理部１４８、ＣＰデータベース１４８ａ、ＳＡＭ管理部１４９、ＳＡＭデータベース１４９ａ、相互認証部１５０および暗号化・復号部１５１を有する。

なお、図１０には、ＥＭＤサービスセンタ１０２内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ１０１との間で送受信されるデータに関連するデータの流れが示されている。

また、図１１には、ＥＭＤサービスセンタ１０２内の機能ブロック相互間のデータの流れのうち、ＳＡＭ105_1～105_4および図１に示す決済機関９１との間で送受信されるデータに関連するデータの流れが示されている。

【００７４】

鍵サーバ１４１は、鍵データベース１４１ａに記憶された各々有効期間が１カ月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部１４８およびＳＡＭ管理部１４９に出力する。

また、鍵データベース１４１ａ配信用鍵データＫＤの他に、記録用鍵データK_{STR}、メディア鍵データK_{MED}およびＭＡＣ鍵データK_{MAC}などの鍵データを記憶する一連の鍵データースからなる。

【００７５】

決算処理部１４２は、ＳＡＭ１０５$_1$～１０５$_4$から入力した利用履歴データ１０８と、証明書・権利書管理部１４５から入力した標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済レポートデータ１０７および決済請求権データ１５２を作成し、決済レポートデータ１０７をコンテンツプロバイダ管理部１４８に出力し、決済請求権データ１５２を決算機関管理部１４４に出力する。

なお、決算処理部１４２は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。

ここで、利用履歴データ１０８は、ユーザホームネットワーク１０３におけるセキュアコンテナ１０４の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部１４２においてセキュアコンテナ１０４に関連したラインセンス料の支払い額を決定する際に用いられる。

【００７６】

利用履歴データ１０８には、例えば、セキュアコンテナ１０４に格納されたコンテンツデータＣの識別子Ｃｏｎｔｅｎｔ＿ＩＤ、セキュアコンテナ１０４を配給したコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、セキュアコンテナ１０４内のコンテンツデータＣの圧縮方法、セキュアコンテナ１０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ１０４を配給を受けたＳＡＭ１０５$_1$～１０５$_4$の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭ１０５$_1$～１０５$_4$のユーザのＵＳＥＲ＿ＩＤなどが記述されている。従って、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク１０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ１０７および決済請求権データ１５２を作成する。当該分配率表は、例えば、セキュアコンテナ１０４に格納されたコンテンツデータ毎に作成される。

また、決済請求権データ１５２は、当該データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った

金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関９１は、決済が終了すると、当該決済機関の利用明細書をＥＭＤサービスセンタ１０２に送る。ＥＭＤサービスセンタ１０２は、当該利用明細書の内容を、対応する権利者に通知する。

【００７７】

決算機関管理部１４４は、決算処理部１４２が生成した決済請求権利データ１５２を図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。

なお、後述するように、決算機関管理部１４４は、決済請求権データ１５２を、コンテンツプロバイダ１０１などの権利者に送信し、権利者自らが、受信した決済請求権データ１５２を用いて決済機関９１に決済を行ってもよい。

また、決算機関管理部１４４は、署名処理部１４３において決済請求権データ１５２のハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いて生成した署名データSIG_{99}を決済請求権データ１５２と共に決済機関９１に送信する。

【００７８】

証明書・権利書管理部１４５は、ＣＥＲデータベース１４５ａに登録されて権威化された公開鍵証明書データCER_{CP}および公開鍵証明書データCER_{SAM1}～CER_{SAM4}などを読み出すと共に、コンテンツプロバイダ１０１の権利書データ１０６およびコンテンツ鍵データＫｃなどをＣＥＲデータベース１４５ａに登録して権威化する。

なお、公開鍵証明書データCER_{SAM1}～CER_{SAM4}を格納するデータベースと、権利書データ１０６およびコンテンツ鍵データＫｃとを個別に設けてもよい。

このとき、証明書・権利書管理部１４５は、例えば、権利書データ１０６およびコンテンツ鍵データＫｃなどのハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いた署名データを付した権威化されたそれぞれの証明書データを作成する。

【００７９】

コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１との間で通信する機能を有し、登録されたコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤなどを管理するＣＰデータベース１４８ａにアクセスできる。

【００８０】

ＳＡＭ管理部１４９は、ユーザホームネットワーク１０３内のＳＡＭ105_1～105_4との間で通信する機能を有し、登録されたＳＡＭの識別子ＳＡＭ＿ＩＤやＳＡＭ登録リストなどを記録したＳＡＭデータベース１４９ａにアクセスできる。

【００８１】

以下、ＥＭＤサービスセンタ１０２内での処理の流れを説明する。

先ず、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１およびユーザホームネットワーク１０３内のＳＡＭ105_1～105_4への配信用鍵データを送信する際の処理の流れを、図１０および図１１を参照しながら説明する。

図１０に示すように、鍵サーバ１４１は、所定期間毎に、例えば、６カ月分の配信用鍵データKD_1～KD_6を鍵データベース１４１ａから読み出してコンテンツプロバイダ管理部１４８に出力する。

また、署名処理部１４３は、配信用鍵データKD_1～KD_6の各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、それぞれに対応する署名データ$SIG_{KD1,ESC}$～$SIG_{KD6,ESC}$を作成し、これをコンテンツプロバイダ管理部１４８に出力する。

コンテンツプロバイダ管理部１４８は、この６カ月分の配信用鍵データKD_1～KD_6およびそれらの署名データ$SIG_{KD1,ESC}$～$SIG_{KD6,ESC}$を、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【００８２】

また、図１１に示すように、鍵サーバ１４１は、所定期間毎に、例えば、３カ月分の配信用鍵データKD_1～KD_3を鍵データベース１４１ａから読み出してＳＡＭ管理部１４９に出力する。

また、署名処理部１４３は、配信用鍵データKD_1～KD_3の各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、それぞれに対応する署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$を作成し、これをＳ

ＡＭ管理部１４９に出力する。

ＳＡＭ管理部１４９は、この３カ月分の配信用鍵データKD_1～KD_3およびそれらの署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$を、相互認証部１５０とＳＡＭ１０５$_1$～１０５$_4$と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、ＳＡＭ１０５$_1$～１０５$_4$に送信する。

【００８３】

以下、ＥＭＤサービスセンタ１０２がコンテンツプロバイダ１０１から、公開鍵証明書データCER_{CP}の発行要求を受けた場合の処理を、図１０および図１２を参照しながら説明する。

図１２は、当該処理のフローチャートである。

ステップＳＣ１：コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、公開鍵データ$K_{CP,P}$および署名データ$SIG_{9,CP}$を含む公開鍵証明書データ発行要求をコンテンツプロバイダ１０１から受信すると、これらを、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。

ステップＳＣ２：当該復号した署名データ$SIG_{9,CP}$の正当性を署名処理部１４３において確認した後に、識別子ＣＰ＿ＩＤおよび公開鍵データ$K_{CP,P}$に基づいて、当該公開鍵証明書データ発行要求を出したコンテンツプロバイダ１０１がＣＰデータベース１４８ａに登録されているか否かを確認する。

【００８４】

ステップＳＣ３：証明書・権利書管理部１４５は、当該コンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}をＣＥＲデータベース１４５ａから読み出してコンテンツプロバイダ管理部１４８に出力する。

【００８５】

ステップＳＣ４：署名処理部１４３は、公開鍵証明書データCER_{CP}のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、署名データ$SIG_{1,ESC}$を作成し、これをコンテンツプロバイダ管理部１４８に出力する。

ステップＳＣ５：コンテンツプロバイダ管理部１４８は、公開鍵証明書データ

ＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$を、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【００８６】

以下、ＥＭＤサービスセンタ１０２がＳＡＭ１０５$_1$から、公開鍵証明書データＣＥＲ$_{SAM1}$の発行要求を受けた場合の処理を、図１１および図１３を参照しながら説明する。

図１３は、当該処理のフローチャートである。

ステップＳＤ１：ＳＡＭ管理部１４９は、ＳＡＭ１０５$_1$の識別子ＳＡＭ$_1$＿ＩＤ、公開鍵データＫ$_{SAM1,P}$および署名データＳＩＧ$_{8,SAM1}$を含む公開鍵証明書データ発行要求をＳＡＭ１０５$_1$から受信すると、これらを、相互認証部１５０とＳＡＭ１０５$_1$と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて復号する。

【００８７】

ステップＳＤ２：当該復号した署名データＳＩＧ$_{8,SAM1}$の正当性を署名処理部１４３において確認した後に、識別子ＳＡＭ$_1$＿ＩＤおよび公開鍵データＫ$_{SAM1,P}$に基づいて、当該公開鍵証明書データの発行要求を出したＳＡＭ１０５$_1$がＳＡＭデータベース１４９ａに登録されているか否かを確認する。

ステップＳＤ３：証明書・権利書管理部１４５は、当該ＳＡＭ１０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$をＣＥＲデータベース１４５ａから読み出してＳＡＭ管理部１４９に出力する。

【００８８】

ステップＳＤ４：署名処理部１４３は、公開鍵証明書データＣＥＲ$_{SAM1}$のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データＫ$_{ESC,S}$を用いて、署名データＳＩＧ$_{50,ESC}$を作成し、これをＳＡＭ管理部１４９に出力する。

ステップＳＤ５：ＳＡＭ管理部１４９は、公開鍵証明書データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{50,ESC}$を、相互認証部１５０とＳＡＭ１０５$_1$と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ＳＡＭ１０５$_1$に送信する。

なお、ＳＡＭ１０５$_2$～１０５$_4$が、公開鍵証明書データを要求した場合の処理は、対象がＳＡＭ１０５$_2$～１０５$_4$に代わるのみで、基本的に上述したＳＡＭ１０５$_1$の場合と同じである。

なお、本発明では、ＥＭＤサービスセンタ１０２は、例えば、ＳＡＭ１０５$_1$の出荷時に、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$および公開鍵データ$K_{SAM1,P}$をＳＡＭ１０５$_1$の記憶部に記憶する場合には、当該出荷時に、公開鍵データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データCER_{SAM1}を、ＳＡＭ１０５$_1$の記憶部に記憶してもよい。

【００８９】

以下、ＥＭＤサービスセンタ１０２が、コンテンツプロバイダ１０１から権利書データ１０６およびコンテンツ鍵データＫｃの登録要求を受けた場合の処理を、図１０および図１４を参照しながら説明する。

図１４は、当該処理のフローチャートである。

ステップＳＥ１：コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１から図７（Ａ）に示す権利書登録要求モジュールＭｏｄ$_2$を受信すると、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて権利書登録要求モジュールＭｏｄ$_2$を復号する。

【００９０】

ステップＳＥ２：署名処理部１４３において、鍵データベース１４１ａから読み出した公開鍵データK_{cp}を用いて、署名データ$SIG_{5,CP}$の正当性を検証する。

ステップＳＥ３：証明書・権利書管理部１４５は、権利書登録要求モジュールＭｏｄ$_2$に格納された権利書データ１０６およびコンテンツ鍵データＫｃを、ＣＥＲデータベース１４５ａに登録する。

【００９１】

以下、ＥＭＤサービスセンタ１０２において決済処理を行なう場合の処理を図１１および図１５を参照しながら説明する。

図１５は、当該処理のフローチャートである。

ステップＳＦ１：ＳＡＭ管理部１４９は、ユーザホームネットワーク１０３の例えばＳＡＭ１０５$_1$ から利用履歴データ１０８およびその署名データＳＩＧ$_{200,SAM1}$を入力すると、利用履歴データ１０８および署名データＳＩＧ$_{200,SAM1}$を、相互認証部１５０とＳＡＭ１０５$_1$ との間の相互認証によって得られたセッション鍵データＫ$_{SES}$ を用いて復号し、ＳＡＭ１０５$_1$ の公開鍵データＫ$_{SAM1}$による署名データＳＩＧ$_{200,SAM1}$の検証を行なった後に、決算処理部１４２に出力する。

【００９２】

ステップＳＦ２：決算処理部１４２は、ＳＡＭ管理部１４９から入力した利用履歴データ１０８と、証明書・権利書管理部１４５を介してＣＥＲデータベース１４５ａから読み出した権利書データ１０６に含まれる標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を生成する。なお、決済請求権データ１５２および決済レポートデータ１０７の生成は、ＳＡＭから利用履歴データ１０８を入力する度に行ってもよいし、所定の期間毎に行ってもよい。

ステップＳＦ３：決算処理部１４２は、決済請求権データ１５２を決算機関管理部１４４に出力する。

決算機関管理部１４４は、決済請求権データ１５２およびその署名データＳＩＧ$_{99}$を、相互認証およびセッション鍵データＫ$_{SES}$ による復号を行なった後に、図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。

これにより、決済請求権データ１５２に示される金額の金銭が、コンテンツプロバイダ１０１に支払われる。

なお、ＥＭＤサービスセンタ１０２は、決済請求権データ１５２をコンテンツプロバイダ１０１に送信し、コンテンツプロバイダ１０１が決済請求権データ１５２を用いて決済記載９１に金銭を請求してもよい。

【００９３】

ステップＳＦ４：決算処理部１４２は、決済レポートデータ１０７をコンテンツプロバイダ管理部１４８に出力する。

決済レポートデータ１０７は、上述したように、例えば、ＥＭＤサービスセンタ１０２が図１に示す決済機関９１に対して行なったコンテンツプロバイダ１０１に関する決済の内容が記述されている。

コンテンツプロバイダ管理部１４８は、決済レポートデータ１０７を、相互認証部１５０と図３に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【００９４】

また、ＥＭＤサービスセンタ１０２は、前述したように、権利書データ１０６を登録（権威化）した後に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に、図７（Ｂ）に示す権威化証明書モジュールMod_{2a}を配信用鍵データKD_1～KD_6で暗号化して送信してもよい。

【００９５】

また、ＥＭＤサービスセンタ１０２は、その他に、$SAM105_1$～105_4の出荷時の処理と、ＳＡＭ登録リストの登録処理とを行なうが、これらの処理については後述する。

【００９６】

〔ユーザホームネットワーク１０３〕

ユーザホームネットワーク１０３は、図１に示すように、ネットワーク機器160_1およびＡ／Ｖ機器160_2～160_4を有している。

ネットワーク機器160_1は、$SAM105_1$を内蔵している。また、ＡＶ機器160_2～160_4は、それぞれ$SAM105_2$～105_4を内蔵している。

$SAM105_1$～105_4の相互間は、例えば、ＩＥＥＥ１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

なお、ＡＶ機器160_2～160_4は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器160_1のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク１０３は、ネットワーク機能を有していない

ＡＶ機器のみを有していてもよい。

【００９７】

以下、ネットワーク機器１６０$_1$について説明する。

図１６ネットワーク機器１６０$_1$の構成図である。

図１６に示すように、ネットワーク機器１６０$_1$は、ＳＡＭ１０５$_1$、通信モジュール１６２、復号・伸長モジュール１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。

【００９８】

ＳＡＭ１０５$_1$～１０５$_4$は、コンテンツ単位の課金処理をおこなうモジュールであり、ＥＭＤサービスセンタ１０２との間で通信を行う。

ＳＡＭ１０５$_1$～１０５$_4$は、例えば、ＥＭＤサービスセンタ１０２によって仕様およびバージョンなどが管理され、家庭機器メーカに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、ＳＡＭ１０５$_1$～１０５$_4$のＩＣ(Integrated Circuit)の内部の仕様を知ることはできず、ＥＭＤサービスセンタ１０２が当該ＩＣのインタフェースなどを統一化し、それに従ってネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$に搭載される。

【００９９】

ＳＡＭ１０５$_1$～１０５$_4$は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Registance)性を持ったハードウェアモジュール（ＩＣモジュールなど）である。

ＳＡＭ１０５$_1$～１０５$_4$の機能をＩＣという形で実現する場合は、ＩＣ内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。ＳＡＭをＩＣという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をＳＡＭとして定義してもよい。

【０１００】

以下、ＳＡＭ１０５$_1$の機能について詳細に説明する。

なお、ＳＡＭ１０５$_2$～１０５$_4$は、ＳＡＭ１０５$_1$と基本的に同じ機能を有している。

図１７は、ＳＡＭ１０５$_1$の機能の構成図である。

なお、図１７には、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力し、セキュアコンテナ１０４内のキーファイルＫＦを復号する処理に関連するデータの流れが示されている。

図１７に示すように、ＳＡＭ１０５$_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、コンテンツプロバイダ管理部１８０、誤り訂正部１８１、ダウンロードメモリ管理部１８２、セキュアコンテナ復号部１８３、復号・伸長モジュール管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、課金処理部１８７、署名処理部１８９、ＳＡＭ管理部１９０、メディアＳＡＭ管理部１９７、スタック（作業）メモリ２００および外部メモリ管理部８１１を有する。

なお、ＡＶ機器１６０$_2$～１６０$_4$はダウンロードメモリ１６７を有していないため、ＳＡＭ１０５$_2$～１０５$_4$にはダウンロードメモリ管理部１８２は存在しない。

【０１０１】

なお、図１７に示すＳＡＭ１０５$_1$の所定の機能は、例えば、図示しないＣＰＵにおいて秘密プログラムを実行することによって実現される。

また、スタックメモリ２００には、以下に示す処理を経て、図１８に示すように、利用履歴データ１０８およびＳＡＭ登録リストが記憶される。

ここで、外部メモリ２０１のメモリ空間は、ＳＡＭ１０５$_1$の外部（例えば、ホストＣＰＵ８１０）からは見ることはできず、ＳＡＭ１０５$_1$のみが外部メモリ２０１の記憶領域に対してのアクセスを管理できる。

外部メモリ２０１としては、例えば、フラッシュメモリあるいは強誘電体メモリ（ＦｅＲＡＭ）などが用いられる。

また、スタックメモリ２００としては、例えばＳＡＲＡＭが用いられ、図１９

に示すように、セキュアコンテナ１０４、コンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOC}、コンテンツプロバイダ１０１の公開鍵証明書CER_{CP}、利用制御状態データ（ＵＣＳ）１６６、およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3などが記憶される。

【０１０２】

以下、$SAM105_1$の機能のうち、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力したときの各機能ブロックの処理内容を図１７を参照しながら説明する。

【０１０３】

相互認証部１７０は、$SAM105_1$がコンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間でオンラインでデータを送受信する際に、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成し、これを暗号化・復号部１７１に出力する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【０１０４】

暗号化・復号部１７１は、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で送受信するデータを、相互認証部１７０が生成したセッション鍵データK_{SES}を用いて暗号化・復号する。

【０１０５】

誤り訂正部１８１は、セキュアコンテナ１０４を誤り訂正してダウンロードメモリ管理部１８２に出力する。

なお、ユーザホームネットワーク１０３は、セキュアコンテナ１０４が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部１８１を、$SAM105_1$に内蔵した場合を例示したが、誤り訂正部１８１の機能を、例えばホストＣＰＵ８１０などの$SAM105_1$の外部に持たせてもよい。

【０１０６】

ダウンロードメモリ管理部１８２は、図１６に示すようにダウンロードメモリ１６７が相互認証機能を持つメディアＳＡＭ１６７ａを有している場合には、相互認証部１７０とメディアＳＡＭ１６７ａとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ１０４を、相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化して図１６に示すダウンロードメモリ１６７に書き込む。ダウンロードメモリ１６７としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図２０に示すように、ＨＤＤ(Hard Disk Drive) などの相互認証機能を備えていないメモリをダウンロードメモリ２１１として用いる場合には、ダウンロードメモリ２１１内はセキュアではないので、コンテンツファイルＣＦをダウンロードメモリ２１１にダウンロードし、機密性の高いキーファイルＫＦを例えば、図１７に示すスタックメモリ２００にダウンロードする。

【０１０７】

セキュアコンテナ復号部１８３は、ダウンロードメモリ管理部１８２から入力したセキュアコンテナ１０４に格納されたキーファイルＫＦを、記憶部１９２から読み出した対応する期間の配信用鍵データKD_1～KD_3を用いて復号し、署名処理部１８９において署名データ$SIG_{2,CP}$～$SIG_{4,CP}$の正当性、すなわちコンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の作成者の正当性を確認した後に、スタックメモリ２００に書き込む。

【０１０８】

ＥＭＤサービスセンタ管理部１８５は、図１に示すＥＭＤサービスセンタ１０２との間の通信を管理する。

【０１０９】

署名処理部１８９は、記憶部１９２から読み出したＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$およびコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、セキュアコンテナ１０４内の署名データの検証を行なう。

【０１１０】

記憶部１９２は、$SAM105_1$の外部から読み出しおよび書き換えできない

秘密データとして、図２１に示すように、配信用鍵データKD_1～KD_3、ＳＡＭ＿ＩＤ、ユーザＩＤ、パスワード、情報参照用ＩＤ、ＳＡＭ登録リスト、記録用鍵データK_{STR}、ルートＣＡの公開鍵データ$K_{R-CA,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、メディア鍵データK_{MED}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ105_1の秘密鍵データ$K_{SAM1,S}$、ＳＡＭ105_1の公開鍵データ$K_{SAM1,P}$を格納した公開鍵証明書CER_{SAM1}、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いた公開鍵証明書CER_{ESC}の署名データSIG_{22}、復号・伸長モジュール１６３との間の相互認証用の元鍵データ、メディアＳＡＭとの間の相互認証用の元鍵データを記憶している。

また、記憶部１９２には、図１７に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部１９２としては、例えば、フラッシュＥＥＰＲＯＭ(Electrically Erasable Programmable RAM)が用いられる。

【０１１１】

以下、ＳＡＭ105_1の処理の流れのうち、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力したときの処理の流れを説明する。

先ず、ＥＭＤサービスセンタ１０２から受信した配信用鍵データKD_1～KD_3を記憶部１９２に格納する際のＳＡＭ105_1内での処理の流れを図１７を参照しながら説明する。

この場合には、先ず、相互認証部１７０と図１０に示す相互認証部１５０との間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データK_{SES}で暗号化された３カ月分の配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$が、ＥＭＤサービスセンタ１０２からＥＭＤサービスセンタ管理部１８５を介してスタックメモリ８１１に書き込まれる。

次に、暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて、配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$が復号される。

次に、署名処理部１８９において、スタックメモリ８１１に記憶された署名デ

ータＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$の正当性が確認された後に、配信用鍵データＫＤ$_1$～ＫＤ$_3$が記憶部１９２に書き込まれる。

【０１１２】

以下、セキュアコンテナ１０４をコンテンツプロバイダ１０１から入力し、セキュアコンテナ１０４内のキーファイルＫＦを復号する際のＳＡＭ１０５$_1$内での処理の流れを図１７および図２２を参照しながら説明する。

図２２は、当該処理のフローチャートである。

ステップＳＧ１：図１７に示すＳＡＭ１０５$_1$の相互認証部１７０と図２に示す相互認証部１２０との間で相互認証が行なわれる。

暗号化・復号部１７１は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、コンテンツプロバイダ管理部１８０を介してコンテンツプロバイダ１０１から受信したセキュアコンテナ１０４を復号する。

【０１１３】

ステップＳＧ２：署名処理部１８９は、図４（Ｃ）に示す署名データＳＩＧ$_{1,ESC}$の検証を行なった後に、図４（Ｃ）に示す公開鍵証明書データＣＥＲ$_{CP}$内に格納されたコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{7,CP}$の正当性を確認する。

コンテンツプロバイダ管理部１８０は、署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{7,CP}$の正当性が確認されると、セキュアコンテナ１０４を誤り訂正部１８１に出力する。

誤り訂正部１８１は、セキュアコンテナ１０４を誤り訂正した後に、ダウンロードメモリ管理部１８２に出力する。

【０１１４】

ステップＳＧ３：ダウンロードメモリ管理部１８２は、相互認証部１７０と図１６に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ１０４をダウンロードメモリ１６７に書き込む。

【０１１５】

ステップＳＧ４：ダウンロードメモリ管理部１８２は、相互認証部１７０と図１６に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュア

コンテナ１０４に格納された図４（Ｂ）に示すキーファイルＫＦをダウンロードメモリ１６７から読み出してセキュアコンテナ復号部１８３に出力する。

そして、セキュアコンテナ復号部１８３は、記憶部１９２から入力した対応する期間の配信用鍵データKD_1～KD_3を用いて、キーファイルＫＦを復号し、図４（Ｂ）に示す署名・証明書モジュールMod_1に格納された署名データ$SIG_{1,ESC}$、$SIG_{2,CP}$～$SIG_{4,CP}$を署名処理部１８９に出力する。

【０１１６】

ステップＳＧ５：署名処理部１８９は、図４（Ｂ）に示す署名データ$SIG_{1,ESC}$の検証を行なった後に、図４（Ｂ）に示す公開鍵証明書データCER_{CP}内に格納された公開鍵データ$K_{ESC,P}$を用いて署名データ$SIG_{2,CP}$～$SIG_{4,CP}$の検証を行なう。これにより、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の作成者の正当性が検証される。

【０１１７】

ステップＳＧ６：セキュアコンテナ復号部１８３は、署名データ$SIG_{2,CP}$～$SIG_{4,CP}$の正当性が確認されると、キーファイルＫＦをスタックメモリ２００に書き込む。

【０１１８】

以下、ダウンロードメモリ１６７にダウンロードされたコンテンツデータＣを利用・購入する処理に関連する各機能ブロックの処理内容を図２３を参照しながら説明する。

【０１１９】

利用監視部１８６は、スタックメモリ２００から権利書データ１０６および利用制御状態データ１６６を読み出し、当該読み出した権利書データ１０６および利用制御状態データ１６６によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ１０６は、図１７を用いて説明したように、復号後にスタックメモリ２００に記憶された図４（Ｂ）に示すキーファイルＫＦ内に格納されている。

また、利用制御状態データ１６６は、後述するように、ユーザによって購入形

態が決定されたときに、スタックメモリ２００に記憶される。

【０１２０】

課金処理部１８７は、図１６に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５に応じた利用履歴データ１０８を作成する。

ここで、利用履歴データ１０８は、前述したように、ユーザによるセキュアコンテナ１０４の購入および利用の形態の履歴を記述しており、ＥＭＤサービスセンタ１０２において、セキュアコンテナ１０４の購入に応じた決済処理およびライインセンス料の支払いを決定する際に用いられる。

【０１２１】

また、課金処理部１８７は、必要に応じて、スタックメモリ２００から読み出した販売価格あるいは標準小売価格データＳＲＰをユーザに通知する。

ここで、販売価格および標準小売価格データＳＲＰは、復号後にスタックメモリ２００に記憶された図４（Ｂ）に示すキーファイルＫＦの権利書データ１０６内に格納されている。

課金処理部１８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御状態データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【０１２２】

また、課金処理部１８７は、操作信号Ｓ１６５に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態（UCS: Usage Control Status)データ１６６を生成し、これをスタックメモリ２００に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ１６６には、コンテンツのＩＤ、購入形態、当該購入形態に応じた価

格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０１２３】

なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に利用制御状態データ１６６をコンテンツデータＣの購入と同時にリアルタイムに送信し、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２に、利用履歴データ１０８を所定の期間内にＳＡＭ１０５$_1$に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ１６６が、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ１６６をコンテンツプロバイダ１０１にリアルタイムに送信する。

【０１２４】

ＥＭＤサービスセンタ管理部１８５は、外部メモリ管理部８１１を介して外部メモリ２０１から読み出した利用履歴データ１０８をＥＭＤサービスセンタ１０２に送信する。

このとき、ＥＭＤサービスセンタ管理部１８５は、署名処理部１８９において、秘密鍵データ$K_{SAM1,s}$を用いて利用履歴データ１０８の署名データ$SIG_{200,SAM1}$を作成し、署名データ$SIG_{200,SAM1}$を利用履歴データ１０８と共にＥＭＤサービスセンタ１０２に送信する。

ＥＭＤサービスセンタ１０２への利用履歴データ１０８の送信は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ１０８に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ２０１の記憶容量に応じて決定される。

【０１２５】

ダウンロードメモリ管理部１８２は、例えば、図１６に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツの再生動作が行われる場合

に、ダウンロードメモリ１６７から読み出したコンテンツデータＣ、スタックメモリ２００から読み出したコンテンツ鍵データＫｃおよび課金処理部１８７から入力したユーザ電子透かし情報用データ１９６を復号・伸長モジュール管理部１８４に出力する。

また、復号・伸長モジュール管理部１８４は、図１６に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツファイルＣＦ、並びにスタックメモリ２００から読み出したコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９を復号・伸長モジュール管理部１８４に出力する。

【０１２６】

ここで、半開示パラメータデータ１９９は、権利書データ１０６内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール１６３では、半開示パラメータデータ１９９に基づいて、暗号化されたコンテンツデータＣを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール１６３がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ１９９によって、コンテンツ鍵データＫｃを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【０１２７】

以下、ＳＡＭ１０５$_1$ 内での処理の流れについて説明する。

先ず、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでの処理の流れを図２３および図２４を参照しながら説明する。

図２４は、当該処理のフローチャートである。

ステップＳＨ１：課金処理部１８７において、ユーザによる図１６に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が発生したか否かが判断され、発生したと判断された場合にはステップＳＨ２の処理が行われ、そうでない場合にはステップＳＨ３の処理が行われる。

【０１２８】

ステップＳＨ２：課金処理部１８７によって、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、復号・伸長モジュール管理部１８４を介して、図１６に示す復号・伸長モジュール１６３に出力される。

このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。

コンテンツファイルＣＦは、図１６に示す復号部２２１において復号された後に、復号部２２２に出力される。

【０１２９】

また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９が、図１６に示す復号・伸長モジュール１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。

次に、電子透かし情報処理部２２４においてユーザ電子透かし情報用データ１９６がコンテンツデータＣに埋め込まれた後、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。

【０１３０】

ステップＳＨ３：ユーザが購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。

ステップＳＨ４：課金処理部１８７において、決定された購入形態に応じた利

用履歴データ１０８および利用制御状態データ１６６が生成され、利用履歴データ１０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に、利用制御状態データ１６６がスタックメモリ２００に書き込まれる。

以後は、利用監視部１８６において、利用制御状態データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【０１３１】

ステップＳＨ５：スタックメモリ２００に格納されているキーファイルＫＦに、利用制御状態データ１６６が加えられ、購入形態が決定した後述する図２９（Ｂ）に示す新たなキーファイルKF_1が生成される。キーファイルKF_1は、スタックメモリ２００に記憶される。

図２９（Ｂ）に示すように、キーファイルKF_1に格納された利用制御状態データ１６６はストレージ鍵データK_{STR}を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{300}が付されている。また、利用制御状態データ１６６およびMAC_{300}からなるモジュールは、メディア鍵データK_{MED}を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データK_{MED}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{301}が付されている。

【０１３２】

以下、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図２３および図２５を参照しながら説明する。

図２５は、当該処理のフローチャートである。

ステップＳＩ１：課金処理部１８７が、ユーザによる操作に応じて、再生を行うコンテンツを指定した操作信号Ｓ１６５を入力する。

ステップＳＩ２：課金処理部１８７は、利用監視部１８６の監視下で、操作信号Ｓ１６５に基づいて、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが読み出される。

【０１３３】

ステップＳＩ３：当該読み出されたコンテンツファイルＣＦが図１６に示す復号・伸長モジュール１６３に出力される。このとき、図２３に示す相互認証部１７０と、図１６に示す復号・伸長モジュール１６３の相互認証部２２０との間で相互認証が行われる。

また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃが復号・伸長モジュール１６３に出力される。

【０１３４】

ステップＳＩ４：復号・伸長モジュール１６３の復号部２２２において、コンテンツ鍵データＫｃを用いたコンテンツファイルＣＦの復号と、伸長部２２３による伸長処理とが行なわれ、再生モジュール１６９において、コンテンツデータＣが再生される。

ステップＳＩ５：課金処理部１８７によって、操作信号Ｓ１６５に応じて、外部メモリ２０１に記憶されている利用履歴データ１０８が更新される。

利用履歴データ１０８は、外部メモリ２０１から読み出された後、相互認証を経て、ＥＭＤサービスセンタ管理部１８５を介して、署名データ$SIG_{200,SAM1}$と共にＥＭＤサービスセンタ１０２に送信される。

【０１３５】

以下、図２６に示すように、例えば、ネットワーク機器160_1のダウンロードメモリ１６７にダウンロードされた既に購入形態が決定されたコンテンツファイルＣＦおよびキーファイルＫＦを、バス１９１を介して、ＡＶ機器160_2の$SAM105_2$に転送する場合の$SAM105_1$内での処理の流れを図２７および図２８を参照しながら説明する。

図２８は、当該処理のフローチャートである。

ステップＳＪ１：ユーザは、購入・利用形態決定操作部１６５を操作して、ダウンロードメモリ１６７に記憶された所定のコンテンツをＡＶ機器160_2に転送することを指示し、当該操作に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。

これにより、課金処理部１８７は、操作信号Ｓ１６５に基づいて、外部メモリ

２０１に記憶されている利用履歴データ１０８を更新する。

【０１３６】

ステップＳＪ２：ダウンロードメモリ管理部１８２は、ダウンロードメモリ１６７から読み出した図２９（Ａ）に示すコンテンツファイルＣＦをＳＡＭ管理部１９０に出力する。

ステップＳＪ３：スタックメモリ２００から読み出した図２９（Ｂ）に示すキーファイルKF_1を、署名処理部１８９およびＳＡＭ管理部１９０に出力する。

ステップＳＪ４：署名処理部１８９は、スタックメモリ２００から読み出したキーファイルKF_1の署名データ$SIG_{42,SAM1}$を作成し、これをＳＡＭ管理部１９０に出力する。

また、ＳＡＭ管理部１９０は、記憶部１９２から、図２９（Ｃ）に示す公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$を読み出す。

【０１３７】

ステップＳＪ５：相互認証部１７０は、$SAM105_2$との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部１７１に出力する。

ＳＡＭ管理部１９０は、図２９（Ａ），（Ｂ），（Ｃ）に示すデータからなる新たなセキュアコンテナを作成する。

ステップＳＪ６：暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて暗号化した後に、図２６に示すＡＶ機器160_2の$SAM105_2$に出力する。

このとき、$SAM105_1$と$SAM105_2$との間の相互認証と並行して、ＩＥＥＥ１３９４シリアルバスであるバス１９１の相互認証が行われる。

【０１３８】

以下、図２６に示すように、$SAM105_1$から入力したコンテンツファイルＣＦなどを、ＲＡＭ型などの記録媒体（メディア）に書き込む際の$SAM105_2$内での処理の流れを、図３０および図３１を参照しながら説明する。

図３１は、当該処理のフローチャートである。

【０１３９】

ステップＳＫ１：$SAM105_2$のＳＡＭ管理部１９０は、図２６に示すよう

に、図２９（Ａ）に示すコンテンツファイルＣＦと、図２９（Ｂ）に示すキーファイルKF_1 およびその署名データ$SIG_{42,SAM1}$ と、図２９（Ｃ）に示す公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とを、ネットワーク機器160_1 の$SAM105_1$ から入力する。

そして、暗号化・復号部１７１において、ＳＡＭ管理部１９０が入力したコンテンツファイルＣＦと、キーファイルKF_1 およびその署名データ$SIG_{42,SAM1}$ と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、相互認証部１７０と$SAM105_1$ の相互認証部１７０との間の相互認証によって得られたセッション鍵データK_{SES} を用いて復号される。

次に、セッション鍵データK_{SES} を用いて復号されたキーファイルKF_1 およびその署名データ$SIG_{42,SAM1}$ と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、スタックメモリ２００に書き込まれる。

【０１４０】

ステップＳＫ２：署名処理部１８９は、スタックメモリ２００から読み出した署名データ$SIG_{22,ESC}$を、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。

そして、署名処理部１８９は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データ$K_{SAM1,P}$を用いて、署名データ$SIG_{42,SAM1}$ の正当を確認する。

次に、署名データ$SIG_{42,SAM1}$ の正当性、すなわちキーファイルKF_1 の作成者の正当性が確認されると、図２９（Ｂ）に示すキーファイルKF_1 をスタックメモリ２００から読み出して暗号化・復号部１７３に出力する。

なお、当該例では、キーファイルKF_1 の作成者と送信元とが同じ場合を述べたが、キーファイルKF_1 の作成者と送信元とが異なる場合には、キーファイルKF_1 に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【０１４１】

ステップＳＫ３：暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データK_{STR} 、メディア鍵データK_{MED} および購入者鍵データK_{PIN} を用い

てキーファイルKF_1を順に暗号化してメディアＳＡＭ管理部１９７に出力する。

なお、メディア鍵データK_{MED}は、図２７に示す相互認証部１７０と図２６に示すＲＡＭ型の記録媒体２５０のメディアＳＡＭ２５２との間の相互認証によって記憶部１９２に事前に記憶されている。

【０１４２】

ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ(Super Audio Compact Disc)、ＤＶＤ(Digital Versatile Disc)機器、ＣＤ－Ｒ機器およびＭＤ(Mini Disc)機器などの種類（当該例では、ＡＶ機器160_2）に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。なお、ＳＡＣＤとＤＶＤとでは、ディスク媒体の物理的な構造が同じであるため、ＤＶＤ機器を用いてＳＡＣＤの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。

【０１４３】

また、メディア鍵データK_{MED}は、記録媒体（当該例では、ＲＡＭ型の記録媒体２５０）にユニークなデータである。

メディア鍵データK_{MED}は、記録媒体（当該例では、図２６に示すＲＡＭ型の記録媒体２５０）側に格納されており、記録媒体のメディアＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアＳＡＭが搭載されている場合には、当該メディアＳＡＭ内に記憶されており、記録媒体にメディアＳＡＭが搭載されていない場合には、例えば、ＲＡＭ領域内のホストＣＰＵ８１０の管理外の領域に記憶されている。

なお、本実施形態のように、機器側のＳＡＭ（当該例では、$SAM105_2$）とメディアＳＡＭ（当該例では、メディアＳＡＭ２５２）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のＳＡＭに転送し、機器側のＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【０１４４】

また、購入者鍵データK_{PIN}は、コンテンツファイルＣＦの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してＥＭＤサービスセンタ１０２によって割り当てられる。購入者鍵データK_{PIN}は、ＥＭＤサービスセンタ１０２において管理される。

【０１４５】

ステップＳＫ４：メディアＳＡＭ管理部１９７は、ＳＡＭ管理部１９０から入力したコンテンツファイルＣＦおよび暗号化・復号部１７３から入力したキーファイルKF_1を、図２６に示す記録モジュール２６０に出力する。

そして、記録モジュール２６０は、メディアＳＡＭ管理部１９７から入力したコンテンツファイルＣＦおよびキーファイルKF_1を、図２６に示すＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１に書き込む。この場合に、キーファイルKF_1を、メディアＳＡＭ２５２内に書き込むようにしてもよい。

【０１４６】

以下、コンテンツの購入形態が未決定の図６に示すＲＯＭ型の記録媒体１３０をユーザホームネットワーク３０３がオフラインで配給を受けた場合に、ＡＶ機器160_2において購入形態を決定する際の処理の流れを図３２、図３３、図３４、図３５を参照しながら説明する。

ステップＳＬ１：ＡＶ機器160_2のＳＡＭ105_2は、先ず、図３３に示す相互認証部１７０と図６に示すＲＯＭ型の記録媒体１３０のメディアＳＡＭ１３３との間で相互認証を行った後に、メディアＳＡＭ１３３からメディア鍵データK_{MED}を入力する。

なお、ＳＡＭ105_2が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。

【０１４７】

ステップＳＬ２：ＲＯＭ型の記録媒体１３０のＲＡＭ領域１３２に記録されているセキュアコンテナ１０４に格納された図４（Ｂ），（Ｃ）に示すキーファイ

ルＫＦおよびその署名データ$ＳＩＧ_{7,CP}$と、公開鍵証明書データ$ＣＥＲ_{CP}$およびその署名データ$ＳＩＧ_{1,ESC}$とが、メディアＳＡＭ管理部１９７を介して入力され、これらがスタックメモリ２００に書き込まれる。

【０１４８】

ステップＳＬ３：署名処理部１８９において、署名データ$ＳＩＧ_{1,ESC}$の正当性を確認した後に、公開鍵証明書データ$ＣＥＲ_{CP}$から公開鍵データ$Ｋ_{CP,P}$を取り出し、この公開鍵データ$Ｋ_{CP,P}$を用いて、署名データ$ＳＩＧ_{7,CP}$の正当性、すなわちキーファイルＫＦの作成者の正当性を検証する。

【０１４９】

ステップＳＬ４：署名処理部１８９において署名データ$ＳＩＧ_{7,CP}$の正当性が確認されると、スタックメモリ２００からセキュアコンテナ復号部１８３に、キーファイルＫＦを読み出す。

そして、セキュアコンテナ復号部１８３において、対応する期間の配信用鍵データ$ＫＤ_{1}$～$ＫＤ_{3}$を用いて、キーファイルＫＦを復号する。

【０１５０】

ステップＳＬ５：署名処理部１８９において、公開鍵データ$Ｋ_{ESC,P}$を用いて、キーファイルＫＦに格納された署名データ$ＳＩＧ_{1,ESCM}$の正当性を確認した後に、キーファイルＫＦ内の公開鍵証明書データ$ＣＥＲ_{CP}$に格納された公開鍵データ$Ｋ_{CP,P}$を用いて、署名データ$ＳＩＧ_{2,CP}$～$ＳＩＧ_{4,CP}$の正当性、すなわちコンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の作成者の正当性を検証する。

【０１５１】

ステップＳＬ６：課金処理部１８７において、ユーザによる図１６に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が発生したか否かが判断され、発生したと判断された場合にはステップＳＬ７の処理が行われ、そうでない場合にはステップＳＬ８の処理が行われる。

【０１５２】

ステップＳＬ７：図３３に示す相互認証部１７０と図３２に示す復号・伸長モジュール１６３との間で相互認証を行った後に、$ＳＡＭ１０５_{2}$の復号・伸長モ

ジュール管理部１８４は、スタックメモリ２００に記憶されているコンテンツ鍵データＫｃおよび権利書データ１０６に格納された半開示パラメータデータ１９９、並びにＲＯＭ型の記録媒体１３０のＲＯＭ領域１３１から読み出したコンテンツデータＣを図３２に示す復号・伸長モジュール１６３に出力する。次に、復号・伸長モジュール１６３において、コンテンツデータＣがコンテンツ鍵データＫｃを用いて半開示モードで復号された後に伸長され、再生モジュール２７０に出力される。そして、再生モジュール２７０において、復号・伸長モジュール１６３からのコンテンツデータＣが試聴モードで再生される。

【０１５３】

ステップＳＬ８：ユーザによる図３２に示す購入形態決定操作部１６５の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号Ｓ１６５が課金処理部１８７に入力される。

【０１５４】

ステップＳＬ９：課金処理部１８７は、操作信号Ｓ１６５に応じた利用制御状態データ１６６を作成し、これをスタックメモリ２００に書き込む。

また、課金処理部１８７は、利用履歴データ１０８を作成あるいは更新する。

【０１５５】

ステップＳＬ１０：スタックメモリ２００から暗号化・復号部１７３に、例えば、図４（Ｂ）に示すキーファイルＫＦに利御制御状態データ１６６を格納した図２９（Ｂ）に示す新たなキーファイルKF_1が出力される。

【０１５６】

ステップＳＬ１１：暗号化・復号部１７３は、スタックメモリ２００から読み出した図２９（Ｂ）に示すキーファイルKF_1を、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化してメディアＳＡＭ管理部１９７に出力する。

【０１５７】

ステップＳＬ１２：図３３に示す相互認証部１７０と図３２に示すメディアＳＡＭ１３３との間で相互認証を行った後に、ＳＡＭ管理部１９７は、暗号化・復号部１７３から入力したキーファイルKF_1を図３２に示す記録モジュール２７

１を介してＲＯＭ型の記録媒体１３０のＲＡＭ領域１３２あるいはメディアＳＡＭ１３３内に書き込む。

これにより、購入形態が決定されたＲＯＭ型の記録媒体１３０が得られる。

このとき、課金処理部１８７が生成した利用制御状態データ１６６および利用履歴データ１０８は、所定のタイミングで、スタックメモリ２００および外部メモリ２０１からそれぞれ読み出しされたＥＭＤサービスセンタ１０２に送信される。

【０１５８】

以下、図３６に示すように、ＡＶ機器160_3において購入形態が未決定のＲＯＭ型の記録媒体１３０からセキュアコンテナ１０４を読み出してＡＶ機器160_2に転送し、ＡＶ機器160_2において購入形態を決定してＲＡＭ型の記録媒体２５０に書き込む際の処理の流れを図３７および図３８を用いて説明する。

図３７は、$SAM105_3$における当該処理のフローチャートである。

図３８は、$SAM105_2$における当該処理のフローチャートである。　なお、ＲＯＭ型の記録媒体１３０からＲＡＭ型の記録媒体２５０へのセキュアコンテナ１０４の転送は、図１に示すネットワーク機器160_1およびＡＶ機器160_1～160_4のいずれの間で行ってもよい。

【０１５９】

ステップＳＭ１１（図３７）：ＡＶ機器160_3のＳＡＭ105_3とＲＯＭ型の記録媒体１３０のメディアＳＡＭ１３３との間で相互認証を行い、ＲＯＭ型の記録媒体１３０のメディア鍵データK_{MED1}をＳＡＭ105_3に転送する。

このとき、同様に、Ｖ機器160_2のＳＡＭ105_2とＲＡＭ型の記録媒体２５０のメディアＳＡＭ２５２との間で相互認証を行い、ＲＡＭ型の記録媒体２５０のメディア鍵データK_{MED2}をＳＡＭ105_2に転送する。

【０１６０】

ステップＳＭ１２：$SAM105_3$は、ＲＡＭ領域１３２から読み出した図４（Ｂ），（Ｃ）キーファイルＫＦ、署名データ$SIG_{7,CP}$、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$とを、図４０に示す暗号化・復号部１７２において、対応する期間の配信用鍵データKD_1～KD_3を用いて順に復

号する。

次に、暗号化・復号部１７２で復号されたコンテンツファイルＣＦは、暗号化・復号部１７１に出力され、ＳＡＭ１０５$_3$と１０５$_2$との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化された後に、ＳＡＭ管理部１９０に出力される。

また、暗号化・復号部１７２で復号されたキーファイルＫＦは、暗号化・復号部１７１および署名処理部１８９に出力される。

【０１６１】

ステップＳＭ１３：署名処理部１８９は、ＳＡＭ１０５$_3$の秘密鍵データ$K_{SAM3,S}$を用いて、キーファイルＫＦの署名データ$SIG_{350,SAM3}$を作成し、これを暗号化・復号部１７１に出力する。

【０１６２】

ステップＳＭ１４：暗号化・復号部１７１は、記憶部１９２から読み出したＳＡＭ１０５$_3$の公開鍵証明書データCER_{SAM3}およびその署名データ$SIG_{351,ESC}$と、キーファイルＫＦおよびその署名データ$SIG_{350,SAM3}$と、ＲＯＭ型の記録媒体１３０のＲＯＭ領域１３１から読み出した図４（Ａ）に示すコンテンツファイルＣＦとを、ＳＡＭ１０５$_3$と１０５$_2$との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化した後に、ＳＡＭ管理部１９０を介して、ＡＶ機器１６０$_2$のＳＡＭ１０５$_2$に出力する。

【０１６３】

ステップＳＮ１（図３８）：ＳＡＭ１０５$_2$では、図４１に示すように、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力されたコンテンツファイルＣＦが、暗号化・復号部１７１においてセッション鍵データK_{SES}を用いて復号された後に、メディアＳＡＭ管理部１９７を介してＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１に書き込まれる。

また、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力されたキーファイルＫＦおよびその署名データ$SIG_{350,SAM3}$と、公開鍵証明書データCER_{SAM3}およびその署名データ$SIG_{351,ESC}$とが、スタックメモリ２００に書き込まれた後に、暗号化・復号部１７１においてセッション鍵データK_{SES}を用いて復号

される。

【０１６４】

ステップＳＮ２：当該復号された署名データ$ＳＩＧ_{351,ECS}$が、署名処理部１８９において署名検証され、その正当性が確認されると、公開鍵証明書データ$ＣＥＲ_{SAM3}$に格納された公開鍵データ$Ｋ_{SAM3}$を用いて、署名データ$ＳＩＧ_{350,SAM3}$の正当性、すなわちキーファイルＫＦの送信元の正当性が確認される。

そして、署名データ$ＳＩＧ_{350,SAM3}$の正当性が確認されると、スタックメモリ２００からキーファイルＫＦが読み出されてセキュアコンテナ復号部１８３に出力される。

【０１６５】

ステップＳＮ３：セキュアコンテナ復号部１８３は、対応する期間の配信用鍵データ$ＫＤ_1$～$ＫＤ_3$を用いて、キーファイルＫＦを復号し、所定の署名検証を経た後に、当該復号したキーファイルＫＦをスタックメモリ２００に書き込む。

その後、スタックメモリ２００に記憶されている既に復号されたキーファイルＫＦに格納された権利書データ１０６が、利用監視部１８６に出力される。そして、利用監視部１８６によって、権利書データ１０６に基づいて、コンテンツの購入形態および利用形態が管理される。

【０１６６】

ステップＳＮ４：課金処理部１８７において、ユーザによる図１６に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が発生したか否かが判断され、発生したと判断された場合にはステップＳＮ５の処理が行われ、そうでない場合にはステップＳＮ６の処理が行われる。

【０１６７】

ステップＳＮ５：ユーザによって試聴モードが選択されると、既にセッション鍵データ$Ｋ_{SES}$で復号されたコンテンツファイルＣＦのコンテンツデータＣと、スタックメモリ２００に記憶されたコンテンツ鍵データＫｃ、権利書データ１０６から得られた半開示パラメータデータ１９９およびユーザ電子透かし情報用データ１９６とが、相互認証を経た後に、図３６に示す復号・伸長モジュール管理部１８４を介して再生モジュール２７０に出力される。そして、再生モジュール

２７０において、試聴モードに対応したコンテンツデータＣの再生が行われる。

【０１６８】

ステップＳＮ６：ユーザによる図３６に示す購入・利用形態決定操作部１６５の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。

ステップＳＮ７：課金処理部１８７において、決定された購入・利用形態に応じて利用制御状態データ１６６および利用履歴データ１０８が生成され、これがスタックメモリ２００および外部メモリ２０１にそれぞれ書き込まれる。

【０１６９】

ステップＳＮ８：スタックメモリ２００から読み出された利用制御状態データ１６６を格納した例えば図２９（Ｂ）に示すキーファイルKF_1が作成され、これが暗号化・復号部１７３に出力される。

ステップＳＮ９：暗号化・復号部１７３において記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED2}および購入者鍵データK_{PIN}を用いて順に暗号化され、メディアＳＡＭ管理部１９７に出力される。

ステップＳＮ１０：メディアＳＡＭ管理部１９７によって、キーファイルKF_1が、図３６に示す記録モジュール２７１によってＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１あるいはメディアＳＡＭ２５２に書き込まれる。

また、利用制御状態データ１６６および利用履歴データ１０８は、所定のタイミングで、ＥＭＤサービスセンタ１０２に送信される。

以下、$SAM105_1$～105_4の実現方法について説明する。

$SAM105_1$～105_4の機能をハードウェアとして実現する場合は、メモリを内蔵したＡＳＩＣ型のＣＰＵを用いて、そのメモリには、図１７に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【０１７０】

例えば、図１７に示す暗号化・復号部１７１などのモジュールは、例えば、処理速度の問題でハードウエアとしてＡＳＩＣ型のＣＰＵ内のＩＰコアとして実装される。クロック速度やＣＰＵコード体系などの性能によっては、暗号化・復号部１７１をソフトウェアとして実装してもよい。

また、図１７に示す記憶部１９２や、図１７に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー（フラッシューＲＯＭ）が用いられ、作業用メモリとしてはＳＲＡＭなどの高速書き込み可能なメモリが用いられる。なお、その他にも、ＳＡＭ105_1～105_4に内蔵されるメモリとして、強誘電体メモリー（ＦｅＲＡＭ）を用いてもよい。

また、ＳＡＭ105_1～105_4には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【０１７１】

上述したように、ＳＡＭ105_1～105_4は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。ＳＡＭ105_1～105_4を搭載した機器のホストＣＰＵのバス経由で、当該ＳＡＭのＩＣ内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、ＳＡＭのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストＣＰＵが割り付けているアドレス空間内に存在しないように、当該ＳＡＭでは、ＣＰＵ側のメモリー空間を管理するＭＭＵ(Memory Magagement Unit)を用いて、搭載機器側のホストＣＰＵからは見えないアドレス空間を設定する。

また、ＳＡＭ105_1～105_4は、Ｘ線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウエアＩＣＥ、ソフトウエアＩＣＥ）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがＩＣ製造後には使用できないような構造をしている。

ＳＡＭ１０５$_1$～１０５$_4$自身は、ハードウエア的な構造においては、メモリを内蔵した通常のＡＳＩＣ型のＣＰＵであり、機能は当該ＣＰＵを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なＡＳＩＣ型のＣＰＵと異なる。

【０１７２】

ＳＡＭ１０５$_1$～１０５$_4$の機能を全てソフトウエアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウエア処理をおこなう場合と、通常のセットに搭載されているホストＣＰＵ上のソフトウエア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがＩＰコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ＩＣＥ（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（ＭｉｎｉＯＳ）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【０１７３】

次に、図１６に示す復号・伸長モジュール１６３について説明する。

図１６に示すように、復号・伸長モジュール１６３は、相互認証部２２０、復号部２２１、復号部２２２、伸長部２２３、電子透かし情報処理部２２４および半開示処理部２２５を有する。

相互認証部２２０は、復号・伸長モジュール１６３がＳＡＭ１０５$_1$からデータを入力する際に、図２６に示す相互認証部１７０との間で相互認証を行ってセッション鍵データK_{SES}を生成する。

【０１７４】

復号部２２１は、ＳＡＭ１０５$_1$から入力したコンテンツ鍵データＫｃ、半開示パラメータデータ１９９、ユーザ電子透かし情報用データ１９６およびコンテ

ンツデータＣを、セッション鍵データK_{SES}を用いて復号する。そして、復号部２２１は、復号したコンテンツ鍵データＫｃおよびコンテンツデータＣを復号部２２２に出力し、復号したユーザ電子透かし情報用データ１９６を電子透かし情報処理部２２４に出力し、半開示パラメータデータ１９９を半開示処理部２２５に出力する。

【０１７５】

復号部２２２は、半開示処理部２２５からの制御に基づいて、コンテンツ鍵データＫｃを用いて、コンテンツデータＣを半開示状態で復号し、復号したコンテンツデータＣを伸長部２２３に出力する。

【０１７６】

伸長部２２３は、復号されたコンテンツデータＣを伸長して、電子透かし情報処理部２２４に出力する。

伸長部２２３は、例えば、図４（Ａ）に示すコンテンツファイルＣＦに格納されたＡ／Ｖ伸長用ソフトウェアを用いて伸長処理を行い、例えば、ＡＴＲＡＣ３方式で伸長処理を行う。

【０１７７】

電子透かし情報処理部２２４は、復号されたユーザ電子透かし情報用データ１９６に応じたユーザ電子透かし情報を、復号されたコンテンツデータＣに埋め込み、新たなコンテンツデータＣを生成する。電子透かし情報処理部２２４は、当該新たなコンテンツデータＣを再生モジュール１６９に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータＣを再生するときに、復号・伸長モジュール１６３において埋め込まれる。

なお、本発明では、コンテンツデータＣにユーザ電子透かし情報用データ１９６を埋め込まないようにしてもよい。

【０１７８】

半開示処理部２２５は、半開示パラメータデータ１９９に基づいて、例えば、コンテンツデータＣのうち復号を行わないブロックと、復号を行うブロックとを復号部２２２に指示する。

また、半開示処理部２２５は、その他に、半開示パラメータデータ１９９に基

づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【０１７９】

再生モジュール１６９は、復号および伸長されたコンテンツデータＣに応じた再生を行う。

【０１８０】

次に、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図４２（Ａ）は、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{50}$が送信される。

モジュールＭｏｄ$_{50}$には、モジュールＭｏｄ$_{51}$およびその秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}が格納されている。

モジュールＭｏｄ$_{51}$には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信するデータＤａｔａとが格納されている。

このように、公開鍵証明書データCER_{CP}を格納したモジュールＭｏｄ$_{50}$を、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に送信することで、ＳＡＭ１０５$_1$において署名データSIG_{CP}の検証を行なう際に、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$に公開鍵証明書データCER_{CP}を送信する必要がなくなる。

【０１８１】

図４２（Ｂ），（Ｃ）は、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に

データＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$ に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$ との間の相互認証によって得たセッション鍵データK_{SES} で暗号化した図４２（Ｂ）に示すモジュールＭｏｄ$_{52}$が送信される。

モジュールＭｏｄ$_{52}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}とが格納されている。

また、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$ には、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$ との間の相互認証によって得たセッション鍵データK_{SES} で暗号化した図４２（Ｃ）に示すモジュールＭｏｄ$_{53}$が送信される。

モジュールＭｏｄ$_{53}$には、コンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}と、その秘密鍵データ$K_{ESC,S}$ による署名データSIG_{ESC} とが格納されている。

【０１８２】

図４２（Ｄ）は、ＳＡＭ１０５$_1$ からコンテンツプロバイダ１０１にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、ＳＡＭ１０５$_1$ からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$ との間の相互認証によって得たセッション鍵データK_{SES} で暗号化したモジュールＭｏｄ$_{54}$が送信される。

モジュールＭｏｄ$_{54}$には、モジュールＭｏｄ$_{55}$およびその秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}が格納されている。

モジュールＭｏｄ$_{55}$には、ＳＡＭ１０５$_1$ の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データ$K_{ESC,S}$ による署名データSIG_{ESC} と、送信するデータＤａｔａとが格納されている。

このように、公開鍵証明書データCER_{SAM1}を格納したモジュールＭｏｄ$_{55}$を、ＳＡＭ１０５$_1$ からコンテンツプロバイダ１０１に送信することで、コンテン

ツプロバイダ１０１において署名データＳＩＧ$_{SAM1}$の検証を行なう際に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に公開鍵証明書データＣＥＲ$_{SAM1}$を送信する必要がなくなる。

【０１８３】

図４２（Ｅ），（Ｆ）は、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データＫ$_{SES}$で暗号化した図４２（Ｅ）に示すモジュールＭｏｄ$_{56}$が送信される。

モジュールＭｏｄ$_{56}$には、送信するデータＤａｔａと、その秘密鍵データＫ$_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$とが格納されている。

また、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１には、ＥＭＤサービスセンタ１０２とコンテンツプロバイダ１０１との間の相互認証によって得たセッション鍵データＫ$_{SES}$で暗号化した図４２（Ｆ）に示すモジュールＭｏｄ$_{57}$が送信される。

モジュールＭｏｄ$_{57}$には、ＳＡＭ１０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$と、その秘密鍵データＫ$_{ESC,S}$による署名データＳＩＧ$_{ESC}$とが格納されている。

【０１８４】

図４３（Ｇ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データＫ$_{SES}$で暗号化したモジュールＭｏｄ$_{58}$が送信される。

モジュールＭｏｄ$_{58}$には、モジュールＭｏｄ$_{59}$およびその秘密鍵データＫ$_{CP,S}$による署名データＳＩＧ$_{CP}$が格納されている。

モジュールＭｏｄ$_{59}$には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データＣＥＲ$_{CP}$と、公開鍵証明書データＣＥＲ$_{CP}$に対しての秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$と、送信するデータＤａｔａとが格納されている。

【０１８５】

図４３（Ｈ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４３（Ｈ）に示すモジュールＭｏｄ$_{60}$が送信される。

モジュールＭｏｄ$_{60}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データＳＩＧ$_{CP}$とが格納されている。

このとき、ＥＭＤサービスセンタ１０２にはコンテンツプロバイダ１０１の公開鍵証明書データＣＥＲ$_{CP}$は既に登録されている。

【０１８６】

図４３（Ｉ）は、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{61}$が送信される。

モジュールＭｏｄ$_{61}$には、モジュールＭｏｄ$_{62}$およびその秘密鍵データ$K_{SAM1,S}$による署名データＳＩＧ$_{SAM1}$が格納されている。

モジュールＭｏｄ$_{62}$には、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データＣＥＲ$_{SAM1}$と、公開鍵証明書データＣＥＲ$_{SAM1}$に対しての秘密鍵データ$K_{ESC,S}$による署名データＳＩＧ$_{ESC}$と、送信するデータＤａｔａとが格納されている。

【０１８７】

図４３（Ｊ）は、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、ＳＡＭ１０５$_1$からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４３（Ｊ）に示すモジュールＭｏｄ$_{63}$が送信される。

モジュールＭｏｄ$_{63}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}とが格納されている。

このとき、ＥＭＤサービスセンタ１０２にはＳＡＭ１０５$_1$の公開鍵証明書データCER_{SAM1}は既に登録されている。

【０１８８】

以下、ＳＡＭ１０５$_1$～１０５$_4$の出荷時におけるＥＭＤサービスセンタ１０２への登録処理について説明する。

なお、ＳＡＭ１０５$_1$～１０５$_4$の登録処理は同じであるため、以下、ＳＡＭ１０５$_1$の登録処理について述べる。

ＳＡＭ１０５$_1$の出荷時には、図１１に示すＥＭＤサービスセンタ１０２の鍵サーバ１４１によって、ＳＡＭ管理部１４９を介して、図１７などに示す記憶部１９２に以下に示す鍵データが初期登録される。

また、ＳＡＭ１０５$_1$には、例えば、出荷時に、記憶部１９２などに、ＳＡＭ１０５$_1$がＥＭＤサービスセンタ１０２に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部１９２には、例えば、図２１において左側に「＊」が付されているＳＡＭ１０５$_1$の識別子ＳＡＭ＿ＩＤ、記録用鍵データK_{STR}、ルート認証局２の公開鍵データK_{R-CA}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$、公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$、復号・伸長モジュール１６３およびメディアＳＡＭとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶

される。

なお、公開鍵証明書データCER_{SAM1}は、$SAM105_1$を出荷後に登録する際にＥＭＤサービスセンタ１０２から$SAM105_1$に送信してもよい。

【０１８９】

ここで、ルート認証局２の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているＲＳＡを使用し、データ長は例えば１０２４ビットである。公開鍵データK_{R-CA}は、図１に示すルート認証局２によって発行される。

また、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$は、短いデータ長でＲＳＡと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば１６０ビットである。但し、暗号化の強度を考慮すると、公開鍵データ$K_{ESC,P}$は１９２ビット以上であることが望ましい。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２に公開鍵データ$K_{ESC,P}$を登録する。

また、ルート認証局９２は、公開鍵データ$K_{ESC,P}$の公開鍵証明書データCER_{ESC}を作成する。公開鍵データ$K_{ESC,P}$を格納した公開鍵証明書データCER_{ESC}は、好ましく、$SAM105_1$の出荷時に記憶部１９２に記憶される。この場合に、公開鍵証明書データCER_{ESC}は、ルート認証局９２の秘密鍵データ$K_{ROOT,S}$で署名されている。

【０１９０】

ＥＭＤサービスセンタ１０２は、乱数を発生して$SAM105_1$の秘密鍵データ$K_{SAM1,S}$、を生成し、これとペアとなる公開鍵データ$K_{SAM1,P}$を生成する。

また、ＥＭＤサービスセンタ１０２は、ルート認証局９２の認証をもらって、公開鍵データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を発行し、これに自らの秘密鍵データ$K_{ESC,S}$を用いて署名データを添付する。すなわち、ＥＭＤサービスセンタ１０２は、セカンドＣＡ（認証局）として機能を果たす。

【０１９１】

また、$SAM105_1$には、図１１に示すＥＭＤサービスセンタ１０２のＳＡＭ管理部１４９により、ＥＭＤサービスセンタ１０２の管理下にある一意（ユニーク）な識別子ＳＡＭ＿ＩＤが割り当てられ、これが$SAM105_1$の記憶部１

９２に格納されると共に、図１１に示すＳＡＭデータベース１４９ａにも格納され、ＥＭＤサービスセンタ１０２によって管理される。

【０１９２】

また、ＳＡＭ１０５$_1$は、出荷後、例えば、ユーザによってＥＭＤサービスセンタ１０２と接続され、登録手続を行うと共に、ＥＭＤサービスセンタ１０２から記憶部１９２に配信用鍵データＫＤ$_1$～ＫＤ$_3$が転送される。

すなわち、ＳＡＭ１０５$_1$を利用するユーザは、コンテンツをダウンロードする前にＥＭＤサービスセンタ１０２に登録手続が必要である。この登録手続は、例えば、ＳＡＭ１０５$_1$を搭載している機器（当該例では、ネットワーク機器１６０$_1$）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

ＳＡＭ１０５$_1$は、上述した登録手続を経た後でないと使用できない。

【０１９３】

ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$のユーザによる登録手続に応じて、ユーザに固有の識別子ＵＳＥＲ＿ＩＤを発行し、例えば、図１１に示すＳＡＭデータベース１４９ａにおいて、ＳＡＭ＿ＩＤとＵＳＥＲ＿ＩＤとの対応関係を管理し、課金時に利用する。

また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$のユーザに対して情報参照用識別子ＩＤと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子ＩＤとパスワードとを用いて、ＥＭＤサービスセンタ１０２に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、ＥＭＤサービスセンタ１０２は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【０１９４】

次に、図２１に示すように、ＳＡＭ１０５$_1$内の記憶部１９２にＳＡＭ登録リストを格納する手順について説明する。

図１に示すＳＡＭ１０５$_1$は、例えば、バス１９１としてＩＥＥＥ１３９４シリアルバスを用いた場合に、バス１９１に接続された機器の電源を立ち上げたり

、新しい機器をバス１９１に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するＳＡＭ１０５$_2$～ＳＡＭ１０５$_4$のＳＡＭ登録リストを得る。

なお、ＩＥＥＥ１３９４シリアルバスであるバス１９１に応じて生成されたトポロジーマップは、例えば、図４４に示すように、バス１９１にＳＡＭ１０５$_1$～１０５$_4$に加えてＡＶ機器１６０$_5$，１６０$_6$のＳＣＭＳ処理回路１０５$_5$，１０５$_6$が接続されている場合に、ＳＡＭ１０５$_1$～１０５$_4$およびＳＣＭＳ処理回路１０５$_5$，１０５$_6$を対象として生成される。

従って、ＳＡＭ１０５$_1$は、当該トポロジーマップから、ＳＡＭ１０５$_1$～１０５$_4$についての情報を抽出してＳＡＭ登録リストを生成する。

【０１９５】

ＳＡＭ登録リストのデータフォーマットは、例えば、図４５に示される。

そして、ＳＡＭ１０５$_1$は、当該ＳＡＭ登録リストを、ＥＭＤサービスセンタ１０２に登録して署名を得る。

これらの処理は、バス１９１のセッションを利用してＳＡＭ１０５$_1$が自動的に行い、ＥＭＤサービスセンタ１０２にＳＡＭ登録リストの登録命令を発行する。

ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$から図４５に示すＳＡＭ登録リストを受けると、有効期限を確認する。そして、ＥＭＤサービスセンタ１０２は、登録時にＳＡＭ１０５$_1$より指定された決済機能の有無を参照して対応する部分の設定を行う。また、ＥＭＤサービスセンタ１０２は、リボケーションリストをチェックしてＳＡＭ登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にＥＭＤサービスセンタ１０２によって使用が禁止されている（無効な）ＳＡＭのリストである。

また、ＥＭＤサービスセンタ１０２は、決済時にはＳＡＭ１０５$_1$に対応するＳＡＭ登録リストを取り出し、その中に記述されたＳＡＭがリボケーションリストに含まれているかを確認する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ登録リストに署名を添付する。

なお、ＳＡＭリボケーションリストは、同一系の（同一のバス１９１に接続さ

れている）ＳＡＭのみを対象として生成され、各ＳＡＭに対応するリボケーションフラグによって、当該ＳＡＭの有効および無効を示している。

【０１９６】

以下、図１に示すコンテンツプロバイダ１０１の全体動作について説明する。

図４６は、コンテンツプロバイダ１０１の全体動作のフローチャートである。

ステップＳ１：ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１が所定の登録処理を経た後に、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をコンテンツプロバイダ１０１に送信する。

また、ＥＭＤサービスセンタ１０２は、$SAM105_1$～105_4が所定の登録処理を経た後に、$SAM105_1$～105_4の公開鍵データ$K_{SAM1,P}$～$K_{SAM4,P}$の公開鍵証明書CER_{CP1}～CER_{CP4}を$SAM105_1$～105_4に送信する。

また、ＥＭＤサービスセンタ１０２は、相互認証を行った後に、各々有効期限が１カ月の６カ月分の配信用鍵データKD_1～KD_6をコンテンツプロバイダ１０１に送信し、３カ月分の配信用鍵データKD_1～KD_3をユーザホームネットワーク１０３に送信する。

このように、ＥＭＤシステム１００では、配信用鍵データKD_1～KD_3を予め$SAM105_1$～105_4に配給しているため、$SAM105_1$～105_4とＥＭＤサービスセンタ１０２との間がオフラインの状態でも、$SAM105_1$～105_4においてコンテンツプロバイダ１０１から配給されたセキュアコンテナ１０４を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ１０８に記述され、利用履歴データ１０８は、$SAM105_1$～105_4とＥＭＤサービスセンタ１０２とが接続されたときに、ＥＭＤサービスセンタ１０２に自動的に送信されるため、ＥＭＤサービスセンタ１０２における決済処理を確実に行うことができる。なお、ＥＭＤサービスセンタ１０２が、所定の期間内に、利用履歴データ１０８を回収できないＳＡＭについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ１６６は、原則として、リアルタイムで、$SAM105_1$～105_4からＥＭＤサービスセンタ１０２に送信される。

【０１９７】

ステップＳ２：コンテンツプロバイダ１０１は、相互認証を行った後に、図７（Ａ）に示す権利登録要求モジュールMod_2を、ＥＭＤサービスセンタ１０２に送信する。

そして、ＥＭＤサービスセンタ１０２は、所定の署名検証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化する。

【０１９８】

ステップＳ３：コンテンツプロバイダ１０１は、対応する期間の配信用鍵データKD_1～KD_6などを用いて暗号化を行って、図４（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびキーファイルＫＦを作成し、これらと図４（Ｃ）に示す公開鍵証明書データCER_{cp}とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、ユーザホームネットワーク１０３に配給する。

【０１９９】

ステップＳ４：ユーザホームネットワーク１０３のＳＡＭ105_1～ＳＡＭ105_4は、セキュアコンテナ１０４を対応する期間の配信用鍵データKD_1～KD_3などを用いて復号し、セキュアコンテナ１０４の作成者および送信者と正当性を検証するための署名検証などを行い、セキュアコンテナ１０４が正当なコンテンツプロバイダ１０１から送信されたか否かを確認する。

【０２００】

ステップＳ５：ＳＡＭ105_1～ＳＡＭ105_4において、ユーザによる図１６に示す購入・利用形態決定操作部１６５の操作に応じた操作信号Ｓ１６５に基づいて、購入・利用形態を決定する。

このとき、図２３に示す利用監視部１８６において、セキュアコンテナ１０４に格納された権利書データ１０６に基づいて、ユーザによるコンテンツファイルＣＦの購入・利用形態が管理される。

【０２０１】

ステップＳ６：ＳＡＭ105_1～ＳＡＭ105_4の図２３に示す課金処理部１８７において、操作信号Ｓ１６５に基づいて、ユーザによる購入・利用形態の決

定の操作を記述した利用履歴データ１０８および利用制御状態データ１６６が生成し、これらをＥＭＤサービスセンタ１０２に送信する。

【０２０２】

ステップＳ７：ＥＭＤサービスセンタ１０２は、図１１に示す決算処理部１４２において、利用履歴データ１０８に基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を作成する。ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データSIG_{99}を、図１に示すペイメントゲートウェイ９０を介して、決済機関９１に送信する。また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０２０３】

ステップＳ８：決済機関９１において、署名データSIG_{99}の検証を行った後に、決済請求権データ１５２に基づいて、ユーザが支払った金額が、コンテンツプロバイダ１０１の所有者に分配される。

【０２０４】

以上説明したように、ＥＭＤシステム１００では、図４に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配給し、セキュアコンテナ１０４内のキーファイルＫＦについての処理を$SAM105_1$～105_4内で行う。

また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データKD_1～KD_3を用いて暗号化されており、配信鍵データKD_1～KD_3を保持している$SAM105_1$～105_4内でのみ復号される。そして、$SAM105_1$～105_4では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。

従って、ＥＭＤシステム１００によれば、ユーザホームネットワーク１０３におけるコンテンツデータＣの購入および利用を、コンテンツプロバイダ１０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。

【０２０５】

また、ＥＭＤシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ１０４を用いて行うことで、ＳＡＭ105_1～105_4におけるコンテンツデータＣの権利処理を双方の場合において共通化できる。

【０２０６】

また、ＥＭＤシステム１００では、ユーザホームネットワーク１０３内のネットワーク機器160_1およびＡＶ機器160_2～160_4においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【０２０７】

第１実施形態の第１変形例

上述した実施形態では、図４（Ｂ）に示すように、コンテンツプロバイダ１０１において配信用鍵データＫＤを用いてキーファイルＫＦを暗号化し、ＳＡＭ105_1～105_4において配信用鍵データＫＤを用いてキーファイルＫＦを復号する場合を例示したが、図１に示すように、コンテンツプロバイダ１０１からＳＡＭ105_1～105_4にセキュアコンテナ１０４を直接供給する場合には、配信用鍵データＫＤを用いたキーファイルＫＦの暗号化は必ずしも行なわなくてもよい。　このように、配信用鍵データＫＤを用いてキーファイルＫＦを暗号化することは、後述する第２実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データＫＤをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第１実施形態の場合でも、配信用鍵データＫＤを用いてキーファイルＫＦを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【０２０８】

また、上述した実施形態では、図４（Ｂ）に示すキーファイルＫＦ内の権利書データ１０６内に標準小売価格データＳＲＰを格納する場合を例示したが、セキュアコンテナ１０４内のキーファイルＫＦの外に、標準小売価格データＳＲＰ（プライスタグデータ）を格納してもよい。この場合には、標準小売価格データＳＲＰに対して秘密鍵データK_{cp}を用いて作成した署名データを添付する。

【０２０９】

第１実施形態の第２変形例

上述した第１実施形態では、図１に示すように、ＥＭＤサービスセンタ１０２が、自らが生成した決済請求権データ１５２を用いて、ペイメントゲートウェイ９０を介して決済機関９１で決済処理を行なう場合を例示したが、例えば、図４７に示すように、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に決済請求権データ１５２を送信し、コンテンツプロバイダ１０１自らが、決済請求権データ１５２を用いて、ペイメントゲートウェイ９０を介して決済機関９１に対して決済処理を行なってもよい。

【０２１０】

第１実施形態の第３変形例

上述した第１実施形態では、単数のコンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ105_1～105_4に、セキュアコンテナ１０４を供給する場合を例示したが、２以上のコンテンツプロバイダ１０１ａ，１０１ｂからＳＡＭ105_1～105_4にそれぞれセキュアコンテナ１０４ａ，１０４ｂを供給するようにしてもよい。

図４８は、コンテンツプロバイダ１０１ａ，１０１ｂを用いる場合の第１実施形態の第３変形例に係わるＥＭＤシステムの構成図である。

この場合には、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１ａおよび１０１ｂに、それぞれ６カ月分の配信用鍵データKDa_1～KDa_6およびKDb_1～KDb_6を配信する。

また、ＥＭＤサービスセンタ１０２は、ＳＡＭ105_1～105_4に、３カ月分の配信用鍵データKDa_1～KDa_3およびKDb_1～KDb_3を配信する。

【０２１１】

そして、コンテンツプロバイダ１０１ａは、独自のコンテンツ鍵データＫｃａを用いて暗号化したコンテンツファイルＣＦａと、コンテンツ鍵データＫｃａおよび権利書データ１０６ａなどを対応する期間の配信用鍵データＫＤａ$_1$～ＫＤａ$_6$を用いて暗号化したキーファイルＫＦａとを格納したセキュアコンテナ１０４ａをＳＡＭ１０５$_1$～１０５$_4$にオンラインおよび／またはオフランで供給する。

このとき、キーファイルの識別子として、ＥＭＤサービスセンタ１０２が配付するグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤが用いられ、ＥＭＤサービスセンタ１０２によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ１０１ｂは、独自のコンテンツ鍵データＫｃｂを用いて暗号化したコンテンツファイルＣＦｂと、コンテンツ鍵データＫｃｂおよび権利書データ１０６ｂなどを対応する期間の配信用鍵データＫＤｂ$_1$～ＫＤｂ$_6$を用いて暗号化したキーファイルＫＦｂとを格納したセキュアコンテナ１０４ｂをＳＡＭ１０５$_1$～１０５$_4$にオンラインおよび／またはオフランで供給する。

【０２１２】

ＳＡＭ１０５$_1$～１０５$_4$は、セキュアコンテナ１０４ａについては、対応する期間の配信用鍵データＫＤａ$_1$～ＫＤａ$_3$を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ１０８ａおよび利用制御状態データ１６６ａをＥＭＤサービスセンタ１０２に送信する。

また、ＳＡＭ１０５$_1$～１０５$_4$は、セキュアコンテナ１０４ｂについては、対応する期間の配信用鍵データＫＤｂ$_1$～ＫＤｂ$_3$を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ１０８ｂおよび利用制御状態データ１６６ｂをＥＭＤサービスセンタ１０２に送信する。

【０２１３】

ＥＭＤサービスセンタ１０２では、利用履歴データ１０８ａに基づいて、コン

テンツプロバイダ１０１ａについての決済請求権データ１５２ａを作成し、これを用いて決済機関９１に対して決済処理を行なう。

また、ＥＭＤサービスセンタ１０２では、利用履歴データ１０８ｂに基づいて、コンテンツプロバイダ１０１ｂについての決済請求権データ１５２ｂを作成し、これを用いて決済機関９１に対して決済処理を行なう。

【０２１４】

また、ＥＭＤサービスセンタ１０２は、権利書データ１０６ａ，１０６ｂを登録して権威化を行なう。このとき、ＥＭＤサービスセンタ１０２は、権利書データ１０６ａ，１０６ｂに対応するキーファイルＫＦａ，ＫＦｂに対して、グローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤを配付する。

また、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１ａ，１０１ｂの公開鍵証明書データCER_{cpa}，CER_{CPb}を発行し、これに自らの署名データ$SIG_{1b,ESC}$，$SIG_{1a,ESC}$を付してその正当性を認証する。

【０２１５】

第２実施形態

上述した実施形態では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ105_1～105_4にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのＳＡＭに配給する場合について説明する。

【０２１６】

図４９は、本実施形態のＥＭＤシステム３００の構成図である。

図４９に示すように、ＥＭＤシステム３００は、コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ユーザホームネットワーク３０３、サービスプロバイダ３１０、ペイメントゲートウェイ９０および決済機関９１を有する。

コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ＳＡＭ305_1～305_4およびサービスプロバイダ３１０は、それぞれ請求項１８および請求項２４などに係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ３０１は、サービスプロバイダ３１０に対してコンテンツデータを供給する点を除いて、前述した第１実施形態のコンテンツプロバイダ１０１と同じである。

また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ１０１およびＳＡＭ５０５$_1$～５０５$_4$に加えて、サービスプロバイダ３１０に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第１実施形態のＥＭＤサービスセンタ１０２と同じである。

また、ユーザホームネットワーク３０３は、ネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$を有している。ネットワーク機器３６０$_1$はＳＡＭ３０５$_1$およびＣＡモジュール３１１を内蔵しており、ＡＶ機器３６０$_2$～３６０$_4$はそれぞれＳＡＭ３０５$_2$～３０５$_4$を内蔵している。

ここで、ＳＡＭ３０５$_1$～３０５$_4$は、サービスプロバイダ３１０からセキュアコンテナ３０４の配給を受ける点と、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０についての署名データの検証処理およびＳＰ用購入履歴データ（データ配給装置用購入履歴データ）３０９の作成を行なう点とを除いて、前述した第１実施形態のＳＡＭ１０５$_1$～１０５$_4$と同じである。

【０２１７】

先ず、ＥＭＤシステム３００の概要について説明する。

ＥＭＤシステム３００では、コンテンツプロバイダ３０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す前述した第１実施形態と同様の権利書(UCP:Usage Control Policy)データ１０６を、高い信頼性のある権威機関であるＥＭＤサービスセンタ３０２に送信する。権利書データ１０６は、ＥＭＤサービスセンタ３０２に登録されて権威化（認証）される。

【０２１８】

また、コンテンツプロバイダ３０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成する。また、コンテンツプロバイダ３０１は、ＥＭＤサービスセンタ３０２から配給された対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_6$を用いて、コンテンツ鍵データＫｃおよび権利書

データ１０６を暗号化し、それらを格納したキーファイルＫＦを作成する。そして、コンテンツプロバイダ３０１は、コンテンツファイルＣＦ、キーファイルＫＦおよび自らの署名データとを格納したセキュアコンテナ１０４を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ３１０に供給する。

【０２１９】

サービスプロバイダ３１０は、コンテンツプロバイダ３０１からセキュアコンテナ１０４を受け取ると、署名データの検証を行なって、セキュアコンテナ１０４が正当なコンテンツプロバイダ３０１によって作成されたものであるか、並びに送り主の正当性を確認する。

次に、サービスプロバイダ３１０は、例えばオフラインで通知されたコンテンツプロバイダ３０１が希望するコンテンツに対しての価格（ＳＲＰ）に、自らのサービスの価格を加算した価格を示すプライスタグデータ（ＰＴ）３１２を作成する。

そして、サービスプロバイダ３１０は、セキュアコンテナ１０４から取り出したコンテンツファイルＣＦおよびキーファイルＫＦと、プライスタグデータ３１２と、これらに対しての自らの秘密鍵データ$K_{SP,S}$による署名データとを格納したセキュアコンテナ３０４を作成する。

このとき、キーファイルＫＦは、配信用鍵データKD_1～KD_6によって暗号化されており、サービスプロバイダ３１０は当該配信用鍵データKD_1～KD_6を保持していないため、サービスプロバイダ３１０はキーファイルＫＦの中身を見たり、書き換えたりすることはできない。

また、ＥＭＤサービスセンタ３０２は、プライスタグデータ３１２を登録して権威化する。

【０２２０】

サービスプロバイダ３１０は、オンラインおよび／またはオフラインでセキュアコンテナ３０４をユーザホームネットワーク３０３に配給する。

このとき、オフラインの場合には、セキュアコンテナ３０４はＳＡＭ305_1～305_4にそのまま供給される。一方、オンラインの場合には、サービスプロ

バイダ３１０とＣＡモジュール３１１との間で相互認証を行い、セキュアコンテナ３０４をサービスプロバイダ３１０においてセッション鍵データK_{SES}を用いた暗号化して送信し、ＣＡモジュール３１１において受信したセキュアコンテナ３０４をセッション鍵データK_{SES}を用いて復号した後に、ＳＡＭ305_1～305_4に転送する。

【０２２１】

次に、ＳＡＭ305_1～305_4において、セキュアコンテナ３０４を、ＥＭＤサービスセンタ３０２から配給された対応する期間の配信用鍵データKD_1～KD_3を用いて復号した後に、署名データの検証処理を行う。

ＳＡＭ305_1～305_4に供給されたセキュアコンテナ３０４は、ネットワーク機器360_1およびＡＶ機器360_2～360_4において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

ＳＡＭ305_1～305_4は、上述したセキュアコンテナ３０４の購入・利用の履歴を利用履歴(Usage Log) データ３０８として記録する。

利用履歴データ（履歴データまたは管理装置用履歴データ）３０８は、例えば、ＥＭＤサービスセンタ３０２からの要求に応じて、ユーザホームネットワーク３０３からＥＭＤサービスセンタ３０２に送信される。

【０２２２】

ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１およびサービスプロバイダ３１０に分配される。

【０２２３】

本実施形態では、第１実施形態と同様に、デジタルのコンテンツデータＣをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを

、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路（配送チャンネル）を介して提供されても、コンテンツデータＣ（商品）を販売するときの最も基本となる商品カプセルである。具体的には、セキュアコンテナは、課金を行うための暗号情報や、コンテンツデータＣの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

【０２２４】

また、本実施形態では、ＥＭＤサービスセンタ３０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、ＥＭＤサービスセンタ３０２は、中立の立場にある最高の権威機関であるルート認証局９２に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ305_1～305_4において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ３０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ３０１の権利書データ１０６およびサービスプロバイダ３１０のプライスタグデータ３１２を登録して権威化することも、ＥＭＤサービスセンタ３０２の認証機能によるものである。

また、ＥＭＤサービスセンタ３０２は、例えば、配信用鍵データKD_1～KD_6などの鍵データの管理を行なう鍵データ管理機能を有する。

また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１が登録した権利書データ１０６とＳＡＭ305_1～ＳＡＭ305_4から入力した利用履歴データ３０８とサービスプロバイダ３１０が登録したプライスタグデータ３１２とに基づいて、ユーザホームネットワーク３０３のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ３０１およびサービスプロバイダ３１０に分配して支払う権利処理（利益分配）機

能を有する。

【０２２５】

以下、コンテンツプロバイダ３０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ３０１〕

図５０は、コンテンツプロバイダ３０１の機能ブロック図であり、サービスプロバイダ３１０との間で送受信されるデータに関連するデータの流れが示されている。

図５０に示すように、コンテンツプロバイダ３０１は、コンテンツマスタソースサーバ１１１、電子透かし情報付加部１１２、圧縮部１１３、暗号化部１１４、乱数発生部１１５、暗号化部１１６、署名処理部１１７、セキュアコンテナ作成部１１８、セキュアコンテナデータベース１１８ａ、記憶部１１９、相互認証部１２０、暗号化・復号部１２１、権利書データ作成部１２２、ＥＭＤサービスセンタ管理部１２５およびサービスプロバイダ管理部３２４を有する。

【０２２６】

図５０において、図２と同一符号を付した構成要素は、前述した第１実施形態において図２および図３を参照しながら説明した同一符号の構成要素と同じである。

すなわち、コンテンツプロバイダ３０１は、図２に示すＳＡＭ管理部１２４の代わりにサービスプロバイダ管理部３２４を設けた構成をしている。

サービスプロバイダ管理部３２４は、セキュアコンテナ作成部１１８から入力したセキュアコンテナ１０４を、オフラインおよび／またはオンラインで、図４９に示すサービスプロバイダ３１０に提供する。セキュアコンテナ１０４には、第１実施形態と同様に、図４（Ａ），（Ｂ），（Ｃ）に示すコンテンツファイルＣＦおよびその署名データ$ＳＩＧ_{6,CP}$と、キーファイルＫＦおよびその署名データ$ＳＩＧ_{7,CP}$と、公開鍵証明書データ$ＣＥＲ_{CP}$およびその署名データ$ＳＩＧ_{1,ESC}$とが格納されている。

【０２２７】

サービスプロバイダ管理部３２４は、セキュアコンテナ１０４をオンラインでサービスプロバイダ３１０に配信する場合には、暗号化・復号部１２１において

セッション鍵データK_{SES}を用いてセキュアコンテナ１０４を暗号化した後に、ネットワークを介してサービスプロバイダ３１０に配信する。

【０２２８】

また、図３に示したコンテンツプロバイダ１０１内でのデータの流れは、サービスプロバイダ３１０にも同様に適用される。

【０２２９】

〔サービスプロバイダ３１０〕

サービスプロバイダ３１０は、コンテンツプロバイダ３０１から提供を受けたセキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦと、自らが生成したプライスタグデータ３１２とを格納したセキュアコンテナ３０４を、オンラインおよび／またはオフラインで、ユーザホームネットワーク３０３のネットワーク機器３６０_1およびＡＶ機器３６０_2～３６０_4に配給する。

サービスプロバイダ３１０によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、ＣＭ（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【０２３０】

図５１は、サービスプロバイダ３１０の機能ブロック図である。

なお、図５１には、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４に応じたセキュアコンテナ３０４をユーザホームネットワーク３０３に供給する際のデータの流れが示されている。

図５１に示すように、サービスプロバイダ３１０は、コンテンツプロバイダ管理部３５０、記憶部３５１、相互認証部３５２、暗号化・復号部３５３、署名処理部３５４、セキュアコンテナ作成部３５５、セキュアコンテナデータベース３５５ａ、プライスタグデータ作成部３５６、ユーザホームネットワーク管理部３５７、ＥＭＤサービスセンタ管理部３５８およびユーザ嗜好フィルタ生成部９２

０を有する。

【０２３１】

以下、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４からセキュアコンテナ３０４を作成し、これをユーザホームネットワーク３０３に配給する際のサービスプロバイダ３１０内での処理の流れを図５１および図５２を参照しながら説明する。

図５２は、当該処理のフローチャートである。

ステップＳＺ１：コンテンツプロバイダ管理部３５０は、オンラインおよび／またはオフラインで、コンテンツプロバイダ３０１から図４に示すセキュアコンテナ１０４の供給を受けてセキュアコンテナ１０４を記憶部３５１に書き込む。

このとき、コンテンツプロバイダ管理部３５０は、オンラインの場合には、図５０に示す相互認証部１２０と図５１に示す相互認証部３５２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテナ１０４を暗号化・復号部３５３において復号した後に、記憶部３５１に書き込む。

【０２３２】

ステップＳＺ２：署名処理部３５４において、記憶部３５１に記憶されているセキュアコンテナ１０４の図４（Ｃ）に示す署名データ$SIG_{1,ESC}$を、記憶部３５１から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$を用いて検証し、その正当性が認められた後に、図４（Ｃ）に示す公開鍵証明書データCER_{CP}から公開鍵データ$K_{CP,P}$を取り出す。

ステップＳＺ３：署名処理部３５４は、当該取り出した公開鍵データ$K_{CP,P}$を用いて、記憶部３５１に記憶されているセキュアコンテナ１０４の図４（Ａ），（Ｂ）に示す署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の検証を行う。

【０２３３】

ステップＳＺ４：プライスタグデータ作成部３５６は、例えばコンテンツプロバイダ３０１からオフラインで通知されたコンテンツプロバイダ３０１が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ３１２を作成し、これをセキュアコンテナ作成部３５５に出力する。

【０２３４】

ステップＳＺ５：署名処理部３５４は、コンテンツファイルＣＦ、キーファイルＫＦおよびプライスタグデータ３１２のハッシュ値をとり、サービスプロバイダ３１０の秘密鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$を作成し、これをセキュアコンテナ作成部３５５に出力する。

【０２３５】

ステップＳＺ６：セキュアコンテナ作成部３５５は、図５３（Ａ）～（Ｄ）に示すように、コンテンツファイルＣＦおよびその署名データ$SIG_{62,SP}$と、キーファイルＫＦおよびその署名データ$SIG_{63,ESC}$と、プライスタグデータ３１２およびその署名データ$SIG_{64,SP}$と、公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$とを格納したセキュアコンテナ３０４を作成し、セキュアコンテナデータベース３５５ａに格納する。そして、セキュアコンテナ作成部３５５は、ユーザホームネットワーク３０３からの要求に応じたセキュアコンテナ３０４をセキュアコンテナデータベース３５５ａから読み出してユーザホームネットワーク管理部３５７に出力する。

このとき、セキュアコンテナ３０４は、複数のコンテンツファイルＣＦと、それらにそれぞれ対応した複数のキーファイルＫＦとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ３０４内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルＣＦを単数のセキュアコンテナ３０４に格納してもよい。これらの複数のコンテンツファイルＣＦなどは、ディレクトリー構造でセキュアコンテナ３０４内に格納してもよい。

【０２３６】

また、セキュアコンテナ３０４は、デジタル放送で送信される場合には、ＭＨＥＧ(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはＸＭＬ／ＳＭＩＬ／ＨＴＭＬ(Hyper TextMarkup Language) プロトコルが用いられる。

このとき、コンテンツファイルＣＦおよびキーファイルＫＦは、コンテンツプロバイダ３０１によって一元的に管理され、セキュアコンテナ３０４を送信する

プロトコルに依存しない。すなわち、コンテンツファイルＣＦおよびキーファイルＫＦは、ＭＨＥＧおよびＨＴＭＬのプロトコルをトンネリングした形でセキュアコンテナ３０４内に格納される。

【０２３７】

ステップＳＺ７：ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４を、オフラインおよび／またはオンラインでユーザホームネットワーク３０３に供給する。

ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４をオンラインでユーザホームネットワーク３０３のネットワーク機器360_1に配信する場合には、相互認証後に、暗号化・復号部３５２においてセッション鍵データK_{SES}を用いてセキュアコンテナ３０４を暗号化した後に、ネットワークを介してネットワーク機器360_1に配信する。

【０２３８】

なお、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４を例えば衛星などを介して放送する場合には、セキュアコンテナ３０４をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}をワーク鍵データK_Wを暗号化し、ワーク鍵データK_Wをマスタ鍵データK_Mを用いて暗号化する。

そして、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４と共に、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを、衛星を介してユーザホームネットワーク３０３に送信する。

また、例えば、マスタ鍵データK_Mを、ＩＣカードなどに記憶してオフラインでユーザホームネットワーク３０３に配給する。

【０２３９】

また、ユーザホームネットワーク管理部３５７は、ユーザホームネットワーク３０３から、当該サービスプロバイダ３１０が配給したコンテンツデータＣに関してのＳＰ用購入履歴データ３０９を受信すると、これを記憶部３５１に書き込む。

サービスプロバイダ３１０は、将来のサービス内容を決定する際に、ＳＰ用購

入履歴データ３０９を参照する。また、ユーザ嗜好フィルタ生成部９２０は、ＳＰ用購入履歴データ３０９に基づいて、当該ＳＰ用購入履歴データ３０９を送信したＳＡＭ305_1～305_4のユーザの嗜好を分析してユーザ嗜好フィルタデータ９００を生成し、これをユーザホームネットワーク管理部３５７を介してユーザホームネットワーク３０３のＣＡモジュール３１１に送信する。

【０２４０】

図５４には、サービスプロバイダ３１０内におけるＥＭＤサービスセンタ３０２との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ３１０の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ３０２に登録処理を行い、グローバルユニークな識別子ＳＰ＿ＩＤを得ている。識別子ＳＰ＿ＩＤは、記憶部３５１に記憶される。

【０２４１】

先ず、サービスプロバイダ３１０が、ＥＭＤサービスセンタ３０２に、自らの秘密鍵データ$K_{SP,S}$に対応する公開鍵データ$K_{SP,S}$の正当性を証明する公開鍵証明書データCER_{SP}を要求する場合の処理を図５４を参照しながら説明する。

先ず、サービスプロバイダ３１０は、真性乱数発生器を用いて乱数を発生して秘密鍵データ$K_{SP,S}$を生成し、当該秘密鍵データ$K_{SP,S}$に対応する公開鍵データ$K_{SP,P}$を作成して記憶部３５１に記憶する。

ＥＭＤサービスセンタ管理部３５８、サービスプロバイダ３１０の識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$を記憶部３５１から読み出す。

そして、ＥＭＤサービスセンタ管理部３５８は、識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$を、ＥＭＤサービスセンタ３０２に送信する。

そして、ＥＭＤサービスセンタ管理部３４８は、当該登録に応じて、公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$をＥＭＤサービスセンタ３０２から入力して記憶部３５１に書き込む。

【０２４２】

次に、サービスプロバイダ３１０が、ＥＭＤサービスセンタ３０２にプライス

タグデータ３１２を登録して権威化する場合の処理を図５４を参照して説明する。

【０２４３】

この場合には、署名処理部３５４において、プライスタグデータ作成部３５６が作成したプライスタグデータ３１２と記憶部３５１から読み出したグローバルユニークな識別子Ｃｏｎｔｅｎｔ＿ＩＤとを格納したモジュールMod_{103}のハッシュ値が求められ、秘密鍵データ$K_{SP,S}$を用いて署名データ$SIG_{80,SP}$が生成される。

また、記憶部３５１から公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$が読み出される。

そして、図５５に示すプライスタグ登録要求用モジュールMod_{102}を、相互認証部３５２とＥＭＤサービスセンタ３０２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部３５３において暗号化した後に、ＥＭＤサービスセンタ管理部３５８からＥＭＤサービスセンタ３０２に送信する。

なお、モジュールMod_{103}に、サービスプロバイダ３１０のグローバルユニークな識別子ＳＰ＿ＩＤを格納してもよい。

【０２４４】

また、ＥＭＤサービスセンタ管理部３５８は、ＥＭＤサービスセンタ３０２から受信した決済レポートデータ３０７ｓを記憶部３５１に書き込む。

【０２４５】

また、ＥＭＤサービスセンタ管理部３５８は、ＥＭＤサービスセンタ３０２から受信したマーケティング情報データ９０４を記憶部３５１に記憶する。

マーケティング情報データ９０４は、サービスプロバイダ３１０が今後配給するコンテンツデータＣを決定する際に参考にされる。

【０２４６】

〔ＥＭＤサービスセンタ３０２〕

ＥＭＤサービスセンタ３０２は、前述したように、認証局（ＣＡ:Certificate Authority）、鍵管理(Key Management)局および権利処理(Rights Clearing) 局

としての役割を果たす。

図５６は、ＥＭＤサービスセンタ３０２の機能の構成図である。

図５６に示すように、ＥＭＤサービスセンタ３０２は、鍵サーバ１４１、鍵データベース１４１ａ、決済処理部４４２、署名処理部４４３、決算機関管理部１４４、証明書・権利書管理部４４５、ＣＥＲデータベース４４５ａ、コンテンツプロバイダ管理部１４８、ＣＰデータベース１４８ａ、ＳＡＭ管理部１４９、ＳＡＭデータベース１４９ａ、相互認証部１５０、暗号化・復号部１５１、サービスプロバイダ管理部３９０、ＳＰデータベース３９０ａ、ユーザ嗜好フィルタ生成部９０１およびマーケティング情報データ生成部９０２を有する。

図５６において、図１０および図１１と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

以下、図５６において、新たな符号を付した機能ブロックについて説明する。

なお、図５６には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ３１０との間で送受信されるデータに関連するデータの流れが示されている。

また、図５７には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ３０１との間で送受信されるデータに関連するデータの流れが示されている。

また、図５８には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、図４９に示すＳＡＭ305_1～305_4および決済機関９１との間で送受信されるデータに関連するデータの流れが示されている。

【０２４７】

決算処理部４４２は、図５８に示すように、ＳＡＭ305_1～305_4から入力した利用履歴データ３０８と、証明書・権利書管理部４４５から入力した標準小売価格データＳＲＰおよびプライスタグデータ３１２に基づいて決済処理を行う。なお、この際に、決済処理部４４２は、サービスプロバイダ３１０によるダンピングの有無などを監視する。

決済処理部４４２は、決済処理により、図５８に示すように、コンテンツプロバイダ３０１についての決済レポートデータ３０７ｃおよび決済請求権データ１

５２ｃを作成し、これらをそれぞれコンテンツプロバイダ管理部１４８および決算機関管理部１４４に出力する。

また、決済処理により、図５６および図５８に示すように、サービスプロバイダ３１０についての決済レポートデータ３０７ｓおよび決済請求権データ１５２ｓを作成し、これらをそれぞれサービスプロバイダ管理部３９０および決算機関管理部１４４に出力する。

ここで、決済請求権データ１５２ｃ，１５２ｓは、当該データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータである。

【０２４８】

ここで、利用履歴データ３０８は、第１実施形態で説明した利用履歴データ１０８と同様に、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。利用履歴データ３０８には、例えば、図５９に示すように、セキュアコンテナ３０４に格納されたコンテンツデータＣの識別子Ｃｏｎｔｅｎｔ＿ＩＤ、セキュアコンテナ３０４に格納されたコンテンツデータＣを提供したコンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、セキュアコンテナ３０４を配給したサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータＣの信号諸元データ、セキュアコンテナ３０４内のコンテンツデータＣの圧縮方法、セキュアコンテナ３０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ３０４を配給を受けたＳＡＭ305_1～305_4の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭ105_1～105_4のユーザのＵＳＥＲ＿ＩＤなどが記述されている。従って、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク３０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【０２４９】

証明書・権利書管理部４４５は、ＣＥＲデータベース４４５ａに登録されて権威化された公開鍵証明書データCER_{cp}、公開鍵証明書データCER_{SP}および公

開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM2}$などを読み出すと共に、コンテンツプロバイダ３０１の権利書データ１０６およびコンテンツ鍵データＫｃ、並びにサービスプロバイダ３１０のプライスタグデータ３１２などをＣＥＲデータベース４４５ａに登録して権威化する。

このとき、証明書・権利書管理部４４５は、権利書データ１０６、コンテンツ鍵データＫｃおよびプライスタグデータ３１２などのハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いた署名データを付して権威化証明書データを作成する。

【０２５０】

コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１との間で通信する機能を有し、登録されているコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤなどを管理するＣＰデータベース１４８ａにアクセスできる。

【０２５１】

ユーザ嗜好フィルタ生成部９０１は、利用履歴データ３０８に基づいて、当該利用履歴データ３０８を送信したＳＡＭ305_1～305_4のユーザの嗜好に応じたコンテンツデータＣを選択するためのユーザ嗜好フィルタデータ９０３を生成し、ユーザ嗜好フィルタデータ９０３をＳＡＭ管理部１４９を介して、当該利用履歴データ３０８を送信したＳＡＭ305_1～305_4に送信する。

【０２５２】

マーケティング情報データ生成部９０２は、利用履歴データ３０８に基づいて、例えば、複数のサービスプロバイダ３１０によってユーザホームネットワーク１０３に配給されたコンテンツデータＣの全体の購入状況などを示すマーケティング情報データ９０４を生成し、これをサービスプロバイダ管理部３９０を介して、サービスプロバイダ３１０に送信する。サービスプロバイダ３１０は、マーケティング情報データ９０４を参考にして、今後提供するサービスの内容を決定する。

【０２５３】

以下、ＥＭＤサービスセンタ３０２内での処理の流れを説明する。

ＥＭＤサービスセンタ３０２からコンテンツプロバイダ３０１への配信用鍵データKD_1～KD_6の送信と、ＥＭＤサービスセンタ３０２からＳＡＭ305_1

～３０５$_4$ への配信用鍵データＫＤ$_1$ ～ＫＤ$_3$ の送信とは、第１実施形態の場合と同様に行なわれる。

【０２５４】

また、ＥＭＤサービスセンタ３０２がコンテンツプロバイダ３０１から、公開鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部４４５がＣＥＲデータベース４４５ａに対して登録を行なう点を除いて、前述した第１実施形態の場合と同様に行なわれる。

【０２５５】

以下、ＥＭＤサービスセンタ３０２がサービスプロバイダ３１０から、公開鍵証明書データの発行要求を受けた場合の処理を、図５６および図６０を参照しながら説明する。

図６０は、当該処理のフローチャートである。

ステップＳＯ１：サービスプロバイダ管理部３９０は、予めＥＭＤサービスセンタ３０２によって与えられたサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、公開鍵データ$K_{SP,P}$および署名データ$SIG_{70,SP}$ を含む公開鍵証明書データ登録要求をサービスプロバイダ３１０から受信すると、これらを、相互認証部１５０と図５１に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES} を用いて復号する。

【０２５６】

ステップＳＯ２：当該復号した署名データ$SIG_{70,SP}$ の正当性を署名処理部４４３において確認した後に、識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ３１０がＳＰデータベース３９０ａに登録されているか否かを確認する。

ステップＳＯ３：証明書・権利書管理部４４５は、当該サービスプロバイダ３１０の公開鍵証明書データCER_{SP}をＣＥＲデータベース４４５ａから読み出してサービスプロバイダ管理部３９０に出力する。

【０２５７】

ステップＳＯ４：署名処理部４４３は、公開鍵証明書データCER_{SP}のハッシュ値をとり、ＥＭＤサービスセンタ３０２の秘密鍵データ$K_{ESC,S}$ を用いて、署

名データＳＩＧ$_{61,ESC}$を作成し、これをサービスプロバイダ管理部３９０に出力する。

ステップＳＯ５：サービスプロバイダ管理部３９０は、公開鍵証明書データＣＥＲ$_{SP}$およびその署名データＳＩＧ$_{61,ESC}$を、相互認証部１５０と図５１に示す相互認証部３５２と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、サービスプロバイダ３１０に送信する。

【０２５８】

なお、ＥＭＤサービスセンタ３０２がＳＡＭ１０５$_1$～１０５$_4$から、公開鍵証明書データの発行要求を受けた場合の処理は、第１実施形態と同様である。

また、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１から権利書データ１０６の登録要求を受けた場合の処理も、第１実施形態と同様である。

【０２５９】

次に、ＥＭＤサービスセンタ３０２が、サービスプロバイダ３１０からプライスタグデータ３１２の登録要求を受けた場合の処理を、図５６および図６１を参照しながら説明する。

図６１は、当該処理のフローチャートである。

ステップＳＰ１：サービスプロバイダ管理部３９０がサービスプロバイダ３１０から図５５に示すプライスタグ登録要求モジュールＭｏｄ$_{102}$を受信すると、相互認証部１５０と図５１に示す相互認証部３５２との間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いてプライスタグ登録要求モジュールＭｏｄ$_{102}$を復号する。

【０２６０】

ステップＳＰ２：当該復号したプライスタグ登録要求モジュールＭｏｄ$_{102}$に格納された署名データＳＩＧ$_{80,SP}$の正当性を署名処理部４４３において確認する。

【０２６１】

ステップＳＰ３：証明書・権利書管理部４４５は、プライスタグ登録要求モジュールＭｏｄ$_{102}$に格納されたプライスタグデータ３１２を、ＣＥＲデータベース４４５ａに登録して権威化する。

【０２６２】

次に、ＥＭＤサービスセンタ３０２において決済を行なう場合の処理を図５８および図６２を参照しながら説明する。

図６２は、当該処理のフローチャートである。

ステップＳＱ１：ＳＡＭ管理部１４９は、ユーザホームネットワーク３０３の例えば$SAM305_1$から利用履歴データ３０８およびその署名データ$SIG_{205,SAM1}$を入力すると、利用履歴データ３０８および署名データ$SIG_{205,SAM1}$を、相互認証部１５０と$SAM305_1$～305_4との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、$SAM305_1$の公開鍵データ$K_{SAM1,P}$を用いて署名データ$SIG_{205,SAM1}$の検証を行なった後に、決算処理部４４２に出力する。

【０２６３】

ステップＳＱ２：決済処理部４４２は、$SAM305_1$から入力した利用履歴データ３０８と、証明書・権利書管理部４４５から入力した標準小売価格データＳＲＰおよびプライスタグデータ３１２とに基づいて決済処理を行う。

決済処理部４４２は、決済処理により、図５８に示すように、コンテンツプロバイダ３０１についての決済レポートデータ３０７ｃおよび決済請求権データ１５２ｃと、サービスプロバイダ３１０についての決済レポートデータ３０７ｓおよび決済請求権データ１５２ｓとを作成する。

なお、決済処理部４４２による決済処理は、利用履歴データ３０８を入力する毎に行ってもよいし、所定の期間毎に行ってもよい。

【０２６４】

ステップＳＱ３：図５６および図５８に示すように、コンテンツプロバイダ３０１およびサービスプロバイダ３１０についての決済請求権データ１５２ｃ，１５２ｓを作成し、これらを決算機関管理部１４４に出力する。

決算機関管理部１４４は、決済請求権データ１５２ｃ，１５２ｓと、それらについて秘密鍵データ$K_{ESC,S}$を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図４９に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。

これにより、決済請求権データ１５２ｃに示される金額の金銭がコンテンツプロバイダ３０１に支払われ、決済請求権データ１５２ｓに示される金額の金銭がサービスプロバイダ３１０に支払われる。

なお、ＥＭＤサービスセンタ３０２は、決済請求権データ１５２ｃ，１５２ｓをそれぞれコンテンツプロバイダ３０１およびサービスプロバイダ３１０に送信してもよい。この場合には、コンテンツプロバイダ３０１およびサービスプロバイダ３１０が、当該受信した決済請求権データ１５２ｃ，１５２ｓに基づいて決済機関９１に金銭を請求する。

【０２６５】

ステップＳＱ４：コンテンツプロバイダ３０１およびサービスプロバイダ３１０についての決済レポートデータＳ３０７ｃ，Ｓ３０７ｓが、それぞれコンテンツプロバイダ管理部１４８およびサービスプロバイダ管理部３９０を介して、コンテンツプロバイダ３０１およびサービスプロバイダ３１０に出力される。

【０２６６】

ＥＭＤサービスセンタ３０２は、その他に、第１実施形態のＥＭＤサービスセンタ１０２と同様に、ＳＡＭ305_1～305_4の出荷時の処理と、ＳＡＭ登録リストの登録処理とを行なう。

【０２６７】

〔ユーザホームネットワーク３０３〕

ユーザホームネットワーク３０３は、図４９に示すように、ネットワーク機器360_1およびＡ／Ｖ機器360_2～360_4を有している。

ネットワーク機器360_1は、ＣＡモジュール３１１およびＳＡＭ305_1を内蔵している。また、ＡＶ機器360_2～360_4は、それぞれＳＡＭ305_2～305_4を内蔵している。

ＳＡＭ305_1～305_4の相互間は、例えば、１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

なお、ＡＶ機器360_2～360_4は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器360_1のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク３０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０２６８】

以下、ネットワーク機器360_1について説明する。

図６３は、ネットワーク機器360_1の構成図である。

図６３に示すように、ネットワーク機器360_1は、通信モジュール１６２、ＣＡモジュール３１１、復号モジュール９０５、$SAM305_1$、復号・伸長モジュール１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。

図６３において、図１６と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。

【０２６９】

通信モジュール１６２は、サービスプロバイダ３１０との間の通信処理を行なう。

具体的には、通信モジュール１６２は、サービスプロバイダ３１０から衛星放送などで受信したセキュアコンテナ３０４を復号モジュール９０５に出力する。また、通信モジュール１６２は、サービスプロバイダ３１０に電話回線などを介してＳＰ用購入履歴データ３０９を受信したユーザ嗜好フィルタデータ９００をＣＡモジュール３１１に出力すると共に、ＣＡモジュール３１１から入力したＳＰ用購入履歴データ３０９を電話回線などを介してサービスプロバイダ３１０に送信する。

【０２７０】

図６４は、ＣＡモジュール３１１および復号モジュール９０５の機能ブロック図である。

図６４に示すように、ＣＡモジュール３１１は、相互認証部９０６、記憶部９０７、暗号化・復号部９０８およびＳＰ用購入履歴データ生成部９０９を有する。

相互認証部９０６は、ＣＡモジュール３１１とサービスプロバイダ３１０との間で電話回線を介してデータを送受信する際に、サービスプロバイダ３１０との

間で相互認証を行ってセッション鍵データK_{SES}を生成し、これを暗号化・復号部９０８に出力する。

【０２７１】

記憶部９０７は、例えば、サービスプロバイダ３１０とユーザとの間で契約が成立した後に、サービスプロバイダ３１０からＩＣカード９１２などを用いてオフラインで供給されたマスタ鍵データK_Mを記憶する。

【０２７２】

暗号化・復号部９０８は、復号モジュール９０５の復号部９１０からそれぞれ暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力し、記憶部９０７から読み出したマスタ鍵データK_Mを用いてワーク鍵データK_Wを復号する。そして、暗号化・復号部９０８は、当該復号したワーク鍵データK_Wを用いてスクランブル鍵データK_{SCR}を復号し、当該復号したスクランブル鍵データK_{SCR}を復号部９１０に出力する。

また、暗号化・復号部９０８は、電話回線などを介して通信モジュール１６２がサービスプロバイダ３１０から受信したユーザ嗜好フィルタデータ９００を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して復号モジュール９０５のセキュアコンテナ選択部９１１に出力する。

また、暗号化・復号部９０８は、ＳＰ用購入履歴データ生成部９０９から入力したＳＰ用購入履歴データ３０９を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して通信モジュール１６２を介してサービスプロバイダ３１０に送信する。

【０２７３】

ＳＰ用購入履歴データ生成部９０９は、図６３に示す購入・利用形態決定操作部１６５を用いてユーザによるコンテンツデータＣの購入操作に応じた操作信号Ｓ１６５、またはＳＡＭ305_1からの利用制御状態データ１６６に基づいて、サービスプロバイダ３１０に固有のコンテンツデータＣの購入履歴を示すＳＰ用購入履歴データ３０９を生成し、これを暗号化・復号部９０８に出力する。

ＳＰ用購入履歴データ３０９は、例えば、サービスプロバイダ３１０が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃

）、契約（更新）情報および購入履歴情報などを含む。

【０２７４】

なお、ＣＡモジュール３１１は、サービスプロバイダ３１０が課金機能を有している場合には、サービスプロバイダ３１０の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、ＣＡモジュール３１１は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ３１０に送信する。

【０２７５】

復号モジュール９０５は、復号部９１０およびセキュアコンテナ選択部９１１を有する。

復号部９１０は、通信モジュール１６２から、それぞれ暗号化されたセキュアコンテナ３０４、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力する。

そして、復号部９１０は、暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_WをＣＡモジュール３１１の暗号化・復号部９０８に出力し、暗号化・復号部９０８から復号されたスクランブル鍵データK_{SCR}を入力する。

そして、復号部９１０は、暗号化されたセキュアコンテナ３０４を、スクランブル鍵データK_{SCR}を用いて復号した後に、セキュアコンテナ選択部９１１に出力する。

【０２７６】

なお、セキュアコンテナ３０４が、MPEG2 Transport Stream 方式でサービスプロバイダ３１０から送信される場合には、例えば、復号部９１０は、TS Packet 内のＥＣＭ(Entitlement Control Message) からスクランブル鍵データK_{SCR}を取り出し、ＥＭＭ(Entitlement Management Message)からワーク鍵データK_Wを取り出す。

ＥＣＭには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、ＥＭＭは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【0277】

セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAモジュール311から入力したユーザ嗜好フィルタデータ900を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択して$SAM305_1$に出力する。

【0278】

次に、$SAM305_1$について説明する。

なお、$SAM305_1$は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図17～図41を用いて前述した第1実施形態の$SAM105_1$と基本的に行なう機能および構造を有している。

また、$SAM305_2$～305_4は、$SAM305_1$と基本的に同じ機能を有している。

すなわち、$SAM305_1$～305_4は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0279】

以下、$SAM305_1$の機能について詳細に説明する。

図65は、$SAM305_1$の機能の構成図である。

なお、図65には、サービスプロバイダ310からセキュアコンテナ304を入力し、セキュアコンテナ304内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図65に示すように、$SAM305_1$は、相互認証部170、暗号化・復号部171，172，173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管理部190、記憶部192、メディアSAM管理部197、スタックメモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部598および外部メモリ管理部811を有する。

なお、図65に示す$SAM305_1$の所定の機能は、$SAM105_1$の場合と

同様に、ＣＰＵにおいて秘密プログラムを実行することによって実現される。

図６５において、図１７と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと同じである。

【０２８０】

また、図６３に示す外部メモリ２０１には、第１実施形態で説明した処理および後述する処理を経て、利用履歴データ３０８およびＳＡＭ登録リストが記憶される。

また、スタックメモリ２００には、図６６に示すように、コンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOC}、コンテンツプロバイダ３０１の公開鍵証明書データCER_{CP}、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}、利用制御状態データ（ＵＣＳ）３６６、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3およびプライスタグデータ３１２などが記憶される。

【０２８１】

以下、$SAM305_1$の機能ブロックのうち、図６５において新たに符号を付した機能ブロックについて説明する。

署名処理部５８９は、記憶部１９２あるいはスタックメモリ２００から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$、コンテンツプロバイダ３０１の公開鍵データ$K_{cp,p}$およびサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$を用いて、セキュアコンテナ３０４内の署名データの検証を行なう。

【０２８２】

課金処理部５８７は、図６７に示すように、図６３に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５と、スタックメモリ２００から読み出されたプライスタグデータ３１２とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

課金処理部５８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御状態データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【０２８３】

また、課金処理部５８７は、課金処理において、利用履歴データ３０８を生成し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。

ここで、利用履歴データ３０８は、第１実施形態の利用履歴データ１０８と同様に、ＥＭＤサービスセンタ３０２において、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。

【０２８４】

また、課金処理部５８７は、操作信号Ｓ１６５に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態（UCS: Usage Control Status）データ１６６を生成し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ１６６には、コンテンツのＩＤ、購入形態、買い切り価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０２８５】

なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ３０５$_1$からサービスプロバイダ３１０に利用制御状態データ１６６をリアルタイムに送信し、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２に、利用履歴データ１０８をＳＡＭ１０５$_1$に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ１６６が、サービスプロバイダ３１０およびＥＭＤサービスセンタ３０２にリアルタイムに送信される。

【０２８６】

また、ＳＡＭ３０５$_1$では、ＥＭＤサービスセンタ管理部１８５がＥＭＤサービスセンタ３０２から受信したユーザ嗜好フィルタデータ９０３が、サービスプロバイダ管理部５８０に出力される。そして、サービスプロバイダ管理部５８０において、図６３に示す復号モジュール９０５から入力したセキュアコンテナ３０４が、ユーザ嗜好フィルタデータ９０３に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ３０４が選択され、当該選択されたセキュアコンテナ３０４が誤り訂正部１８１に出力される。これにより、ＳＡＭ３０５$_1$において、当該ＳＡＭ３０５$_1$のユーザが契約している全てのサービスプロバイダ３１０を対象として、当該ユーザによるコンテンツデータＣの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータＣの選択処理が可能になる。

【０２８７】

以下、ＳＡＭ３０５$_1$内での処理の流れを説明する。

ＥＭＤサービスセンタ３０２から受信した配信用鍵データＫＤ$_1$～ＫＤ$_3$を記憶部１９２に格納する際のＳＡＭ３０５$_1$内での処理の流れは、前述したＳＡＭ１０５$_1$の場合と同様である。

【０２８８】

以下、セキュアコンテナ３０４をサービスプロバイダ３１０から入力し、セキュアコンテナ３０４内のキーファイルＫＦを復号する際のＳＡＭ３０５$_1$内での処理の流れを図６５および図６８を参照しながら説明する。

図６８は、当該処理のフローチャートである。

ステップＳＲ１：相互認証部１７０と図５１に示すサービスプロバイダ３１０の相互認証部３５２との間で相互認証が行なわれる。

暗号化・復号部１７１は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、サービスプロバイダ管理部５８０を介してサービスプロバイダ３１０から受信した図５３に示すセキュアコンテナ３０４を復号する。

【０２８９】

ステップＳＲ２：署名処理部５８９は、図５３（Ｄ）に示す署名データＳＩＧ

$61,ESC$の検証を行なった後に、図５３（Ｄ）に示す公開鍵証明書データCER_{SP}内に格納されたサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$の正当性を確認する。

サービスプロバイダ管理部５８０は、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$の正当性が確認されると、セキュアコンテナ３０４を誤り訂正部１８１に出力する。

誤り訂正部１８１は、セキュアコンテナ３０４を誤り訂正した後に、ダウンロードメモリ管理部１８２に出力する。

【０２９０】

ステップＳＲ３：ダウンロードメモリ管理部１８２は、相互認証部１７０と図６３に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ３０４をダウンロードメモリ１６７に書き込む。

【０２９１】

ステップＳＲ４：ダウンロードメモリ管理部１８２は、相互認証部１７０と図６３に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ３０４に格納された図５３（Ｂ）に示すキーファイルＫＦを読み出してセキュアコンテナ復号部１８３に出力する。

そして、セキュアコンテナ復号部１８３は、記憶部１９２から入力した対応する期間の配信用鍵データKD_1～KD_3を用いて、キーファイルＫＦを復号する。

【０２９２】

ステップＳＲ５：セキュアコンテナ復号部１８３は、図５３（Ｂ）に示す署名・証明書モジュールMod_1に格納された署名データ$SIG_{1,ESC}$、$SIG_{2,cp}$～$SIG_{4,cp}$を署名処理部５８９に出力する。

署名処理部５８９は、図５３（Ｂ）に示す署名データ$SIG_{1,ESC}$の検証を行なった後に、公開鍵証明書データCER_{cp}内に格納された公開鍵データ$K_{CP,P}$を用いて署名データ$SIG_{2,cp}$～$SIG_{4,cp}$の検証を行なう。

【０２９３】

ステップＳＲ６：セキュアコンテナ復号部１８３は、署名データ$SIG_{2,cp}$～

$SIG_{4,cp}$の正当性が確認されると、キーファイルＫＦをスタックメモリ２００に書き込む。

【０２９４】

以下、サービスプロバイダ３１０からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ３０４の購入形態を決定するまでの処理の流れを図６７および図６９を参照しながら説明する。

図６９は、当該処理のフローチャートである。

ステップＳＳ１：課金処理部５８７において、ユーザによる図６３に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が入力されたか否かが判断あれ、入力されたと判断された場合にはステップＳＳ２の処理が実行され、そうでない場合にはステップＳＳ３の処理が実行される。

【０２９５】

ステップＳＳ２：例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、復号・伸長モジュール管理部１８４を介して、図６３に示す復号・伸長モジュール１６３に出力される。

このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。

コンテンツファイルＣＦは、図６３に示す復号部２２１において復号された後に、復号部２２２に出力される。

【０２９６】

また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９が、図６３に示す復号・伸長モジュール１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ１９９が半開示処理部２２５に出力

され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。

次に、電子透かし情報処理部２２４においてユーザ電子透かし情報用データ１９６がコンテンツデータＣに埋め込まれた後、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。

【０２９７】

ステップＳＳ３：コンテンツを試聴したユーザが、購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。

【０２９８】

ステップＳＳ４：課金処理部１８７において、決定された購入形態に応じた利用履歴データ３０８および利用制御状態データ１６６が生成され、利用履歴データ３０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に利用制御状態データ１６６がスタックメモリ２００に書き込まれる。

以後は、利用監視部１８６において、利用制御状態データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【０２９９】

ステップＳＳ５：スタックメモリ２００に格納されているキーファイルＫＦに、利用制御状態データ１６６が加えられ、購入形態が決定した後述する図７１に示す新たなキーファイルKF_{11}が生成される。キーファイルKF_{11}は、スタックメモリ２００に記憶される。

図７１に示すように、キーファイルKF_1に格納された利用制御状態データ１６６はストレージ鍵データK_{STR}を用いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{300}が付されている。また、利用制御状態データ１６６およびMAC_{300}からなるモジュールは、メディア鍵データ$_{MED}$を用

いてＤＥＳのＣＢＣモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データK_{MED}をＭＡＣ鍵データとして用いて生成したＭＡＣ値であるMAC_{301}が付されている。

【０３００】

次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図６７および図７０を参照しながら説明する。

図７０は、当該処理のフローチャートである。

ステップＳＴ１：例えば、ユーザによる操作に応じて、再生対象となるコンテンツの指定をＳＡＭが受ける。

【０３０１】

ステップＳＴ２：利用監視部１８６の監視下で、操作信号Ｓ１６５に基づいて、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが読み出される。

ステップＳＴ３：当該読み出されたコンテンツファイルＣＦが、図６３に示す復号・伸長モジュール１６３に出力される。

また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃが復号・伸長モジュール１６３に出力される。

【０３０２】

ステップＳＴ４：復号・伸長モジュール１６３の復号部２２２において、コンテンツ鍵データＫｃを用いたコンテンツファイルＣＦの復号と、伸長部２２３による伸長処理とが行なわれ、再生モジュール１６９において、コンテンツデータＣが再生される。

ステップＳＴ５：課金処理部５８７において、操作信号Ｓ１６５に応じて、利用履歴データ３０８が更新される。

利用履歴データ３０８は、秘密鍵データ$K_{SAM1,S}$を用いて作成したそれぞれ署名データ$SIG_{205,SAM1}$と共に、ＥＭＤサービスセンタ管理部１８５を介して、所定のタイミングで、ＥＭＤサービスセンタ３０２に送信される。

【０３０３】

以下、図７２に示すように、例えば、ネットワーク機器３６０$_1$のダウンロードメモリ１６７にダウンロードされた既に購入形態が決定されたコンテンツファイルＣＦを、バス１９１を介して、ＡＶ機器３６０$_2$のＳＡＭ３０５$_2$に転送する場合のＳＡＭ３０５$_1$内での処理の流れを図７３および図７４を参照しながら説明する。

ステップＳＵ１：ユーザは、購入・利用形態決定操作部１６５を操作して、ダウンロードメモリ１６７に記憶された所定のコンテンツをＡＶ機器３６０$_2$に転送することを指示し、当該操作に応じた操作信号Ｓ１６５が、課金処理部５８７に出力される。

これにより、課金処理部５８７は、操作信号Ｓ１６５に基づいて、スタックメモリ２００に記憶されている利用履歴データ３０８を更新する。

【０３０４】

ステップＳＵ２：ダウンロードメモリ管理部１８２は、ダウンロードメモリ１６７から読み出した図７５（Ａ）に示すコンテンツファイルＣＦをＳＡＭ管理部１９０に出力する。

ステップＳＵ３：スタックメモリ２００から読み出した図７５（Ｂ）に示す既に購入形態が決定されたキーファイルKF_{11}を、署名処理部５８９およびＳＡＭ管理部１９０に出力する。

ステップＳＵ４：署名処理部５８９は、キーファイルKF_{11}の署名データ$SIG_{80,SAM1}$を作成し、これをＳＡＭ管理部１９０に出力する。

【０３０５】

ステップＳＵ５：ＳＡＭ管理部１９０は、記憶部１９２から、図７５（Ｃ）に示す公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$を読み出す。

また、相互認証部１７０は、ＳＡＭ３０５$_2$との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部１７１に出力する。

ＳＡＭ管理部１９０は、図７５（Ａ），（Ｂ），（Ｃ）に示すデータからなるセキュアコンテナを作成する。

【０３０６】

ステップＳＵ６：暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて当該セキュアコンテナを暗号化して作成して、図７３に示すＡＶ機器３６０$_2$のＳＡＭ３０５$_2$に出力する。

【０３０７】

以下、図７２に示すように、ＳＡＭ３０５$_1$から入力したコンテンツファイルＣＦなどを、ＲＡＭ型などの記録媒体（メディア）に書き込む際のＳＡＭ３０５$_2$内での処理の流れを、図７６および図７７を参照しながら説明する。

図７７は、当該処理のフローチャートである。

【０３０８】

ステップＳＶ１：ＳＡＭ３０５$_2$のＳＡＭ管理部１９０は、図７６に示すように、図７５（Ａ）に示すコンテンツファイルＣＦ、図７５（Ｂ）に示すキーファイルKF_{11}およびその署名データ$SIG_{80,SAM1}$と、図７５（Ｃ）に示す公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とを、ネットワーク機器３６０$_1$のＳＡＭ３０５$_1$から入力する。

そして、暗号化・復号部１７１において、ＳＡＭ管理部１９０が入力したコンテンツファイルＣＦと、キーファイルKF_{11}およびその署名データ$SIG_{80,SAM1}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、相互認証部１７０とＳＡＭ３０５$_1$の相互認証部１７０との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号される。

【０３０９】

次に、セッション鍵データK_{SES}を用いて復号されたコンテンツファイルＣＦがメディアＳＡＭ管理部１９７に出力される。

また、セッション鍵データK_{SES}を用いて復号されたキーファイルKF_{11}およびその署名データ$SIG_{80,SAM1}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、スタックメモリ２００に書き込まれる。

【０３１０】

ステップＳＶ２：署名処理部５８９は、スタックメモリ２００から読み出した署名データ$SIG_{22,ESC}$を、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$

を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。

そして、署名処理部５８９は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データ$K_{SAM1,P}$を用いて、署名データ$SIG_{80,SAM1}$の正当性を確認する。

【０３１１】

ステップＳＶ３：署名データ$SIG_{80,SAM1}$の正当性を確認されると、図７５（Ｂ）に示すキーファイルKF_{11}をスタックメモリ２００から読み出して暗号化・復号部１７３に出力する。

そして、暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いてキーファイルKF_{11}を順に暗号化してメディアＳＡＭ管理部１９７に出力する。

【０３１２】

ステップＳＶ４：メディアＳＡＭ管理部１９７は、ＳＡＭ管理部１９０から入力したコンテンツファイルＣＦおよび暗号化・復号部１７３から入力したキーファイルKF_{11}を、図７２に示す記録モジュール２６０に出力する。

そして、記録モジュール２６０は、メディアＳＡＭ管理部１９７から入力したコンテンツファイルＣＦおよびキーファイルKF_{11}を、図７２に示すＲＡＭ型の記録媒体２５０のＲＡＭ領域２５１に書き込む。

【０３１３】

なお、$SAM305_1$内での処理のうち、コンテンツの購入形態が未決定のＲＯＭ型の記録媒体の購入形態を決定する際の$AV機器360_2$内での処理の流れ、$AV機器360_3$において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナ３０４を読み出してこれを$AV機器360_2$に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ３１０の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ３１２を格納する点を除いて、第１実施形態の$SAM105_1$の場合と同じである。

【０３１４】

次に、図４９に示すＥＭＤシステム３００の全体動作について説明する。

図７８および図７９は、ＥＭＤシステム３００の全体動作のフローチャートである。

ここでは、サービスプロバイダ３１０からユーザホームネットワーク３０３にオンラインでセキュアコンテナ３０４を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、ＥＭＤサービスセンタ３０２へのコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ305_1～305_4の登録は既に終了しているものとする。

【０３１５】

ステップＳ２１：ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}を、自らの署名データ$SIG_{1,ESC}$と共にコンテンツプロバイダ３０１に送信する。

また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データ$K_{SP,P}$の公開鍵証明書CER_{SP}を、自らの署名データ$SIG_{61,ESC}$と共にサービスプロバイダ３１０に送信する。

また、ＥＭＤサービスセンタ３０２は、各々有効期限が１カ月の６カ月分の配信用鍵データKD_1～KD_6をコンテンツプロバイダ３０１に送信し、３カ月分の配信用鍵データKD_1～KD_3をユーザホームネットワーク３０３のＳＡＭ305_1～305_4に送信する。

【０３１６】

ステップＳ２２：コンテンツプロバイダ３０１は、図７（Ａ）に示す権利登録要求モジュールMod_2を、ＥＭＤサービスセンタ３０２に送信する。

そして、ＥＭＤサービスセンタ３０２は、所定の署名検証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化（認証）する。

【０３１７】

ステップＳ２３：コンテンツプロバイダ３０１は、署名データの作成処理や、ＳＩＧ対応する期間の配信用鍵データKD_1～KD_3などを用いた暗号化処理を経て、図４（Ａ），（Ｂ），（Ｃ）に示すデータを格納したセキュアコンテナ１０４を、サービスプロバイダ３１０に供給する。

【０３１８】

ステップＳ２４：サービスプロバイダ３１０は、図４（Ｃ）に示す署名データ$ＳＩＧ_{1,ESC}$を検証した後に、公開鍵証明書データ$ＣＥＲ_{CP}$に格納された公開鍵データ$K_{CP,P}$を用いて、図４（Ａ），（Ｂ）に示す署名データ$ＳＩＧ_{6,CP}$および$ＳＩＧ_{7,CP}$を検証して、セキュアコンテナ１０４が正当なコンテンツプロバイダ３０１から送信されたものであるかを確認する。

【０３１９】

ステップＳ２５：サービスプロバイダ３１０は、プライスタグデータ３１２を作成し、プライスタグデータ３１２を格納した図５３に示すセキュアコンテナ３０４を作成する。

【０３２０】

ステップＳ２６：サービスプロバイダ３１０は、図５５に示すプライスタグ登録要求モジュール$Ｍｏｄ_{102}$を、ＥＭＤサービスセンタ３０２に送信する。

そして、ＥＭＤサービスセンタ３０２は、所定の署名検証を行った後に、プライスタグデータ３１２を登録して権威化する。

【０３２１】

ステップＳ２７：サービスプロバイダ３１０は、例えば、ユーザホームネットワーク３０３のＣＡモジュール３１１からの要求に応じて、ステップＳ２５で作成したセキュアコンテナ３０４を、オンラインあるいはオフラインで、図６３に示すネットワーク機器３６０_{1}の復号モジュール９０５に送信する。

【０３２２】

ステップＳ２８：ＣＡモジュール３１１は、ＳＰ用購入履歴データ３０９を作成し、これを所定のタイミングで、サービスプロバイダ３１０に送信する。

【０３２３】

ステップＳ２９：$ＳＡＭ３０５_{1}$～３０５_{4}のいずれかにおいて、図５３（Ｄ）に示す署名データ$ＳＩＧ_{61,ESC}$を検証した後に、公開鍵証明書データ$ＣＥＲ_{SP}$に格納された公開鍵データ$K_{SP,P}$を用いて、図５３（Ａ），（Ｂ），（Ｃ）に示す署名データ$ＳＩＧ_{62,SP}$、$ＳＩＧ_{63,SP}$，$ＳＩＧ_{64,SP}$を検証して、セキュアコンテナ３０４が正当なサービスプロバイダ３１０から送信されたものであるか

を確認する。

【０３２４】

ステップＳ３０：ＳＡＭ３０５$_1$～３０５$_4$のいずれかにおいて、配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて、図５３（Ｂ）に示すキーファイルＫＦを復号する。そして、ＳＡＭ３０５$_1$～３０５$_4$のいずれかにおいて、図５３（Ｂ）に示す署名データＳＩＧ$_{1,ESC}$を検証した後に、公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{CP,P}$を用いて、図５３（Ｂ）に示す署名データＳＩＧ$_{2,CP}$，ＳＩＧ$_{3,CP}$およびＳＩＧ$_{4,CP}$を検証して、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６が正当なコンテンツプロバイダ３０１によって作成されたものであるかを確認する。

【０３２５】

ステップＳ３１：ユーザが図６３の購入・利用形態決定操作部１６５を操作してコンテンツの購入・利用形態を決定する。

【０３２６】

ステップＳ３２：ステップＳ３１において生成された操作信号Ｓ１６５に基づいて、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４の利用履歴（Usage Log）データ３０８が生成される。

ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８およびその署名データＳＩＧ$_{205,SAM1}$が送信される。

【０３２７】

ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、決済請求権データ１５２ｃ，１５２ｓを作成する。

【０３２８】

ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓを自らの署名データと共に送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の

所有者に分配される。

【０３２９】

以上説明したように、ＥＭＤシステム３００では、図４に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ３０１からサービスプロバイダ３１０に配給し、セキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦをそのまま格納したセキュアコンテナ３０４をサービスプロバイダ３１０からユーザホームネットワーク３０３に配給し、キーファイルＫＦについての処理をＳＡＭ305_1～305_4内で行う。

また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データKD_1～KD_3を用いて暗号化されており、配信鍵データKD_1～KD_3を保持しているＳＡＭ305_1～305_4内でのみ復号される。そして、ＳＡＭ305_1～305_4では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。

【０３３０】

従って、ＥＭＤシステム３００によれば、ユーザホームネットワーク３０３におけるコンテンツデータＣの購入および利用を、サービスプロバイダ３１０における処理とは無関係に、コンテンツプロバイダ１０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。すなわち、ＥＭＤシステム３００にれば、権利書データ１０６をサービスプロバイダ３１０が管理できないようできる。

そのため、ＥＭＤシステム３００によれば、異系列の複数のサービスプロバイダ３１０を介してユーザホームネットワーク３０３にコンテンツデータＣが配給された場合でも、ユーザホームネットワーク３０３における当該コンテンツデータＣについての権利処理を、コンテンツプロバイダ３０１が作成した共通の権利書データ１０６に基づいて行わせることができる。

【０３３１】

また、ＥＭＤシステム３００では、サービスプロバイダ３１０からユーザホームネットワーク１０３へのコンテンツデータＣの配給を、オンラインおよびオフ

ラインの何れの場合でもセキュアコンテナ３０４を用いて行うことで、双方の場合において、ＳＡＭ３０$５_1$～３０$５_4$におけるコンテンツデータＣの権利処理を共通化できる。

【０３３２】

また、ＥＭＤシステム３００では、ユーザホームネットワーク３０３内のネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【０３３３】

また、ＥＭＤシステム３００によれば、ＥＭＤサービスセンタ３０２が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ３０１およびＥＭＤサービスセンタ３０２の所有者に、予め決められた比率に従って確実に分配される。

また、ＥＭＤシステム３００によれば、同じコンテンツプロバイダ３０１が供給した同じコンテンツファイルＣＦについての権利書データ１０６は、サービスプロバイダ３１０のサービス形態とは無関係に、そのままＳＡＭ３０$５_1$～３０$５_4$に供給される。従って、ＳＡＭ３０$５_1$～３０$５_4$において、権利書データ１０６に基づいて、コンテンツプロバイダ３０１の意向通りに、コンテンツファイルＣＦの利用を行わせることができる。

すなわち、ＥＭＤシステム３００によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織７２５に頼ることなく、技術的な手段によって、コンテンツプロバイダ３０１の所有者の権利および利益を確実に守ることができる。

【０３３４】

第２実施形態の第１変形例

図８０は、第２実施形態の第１変形例に係わる２個のサービスプロバイダを用いたＥＭＤシステム３００ａの構成図である。

図８０において、図４９と同一符号を付した構成要素は、第２実施形態で説明

した同一符号の構成要素と同じである。

図８０に示すように、ＥＭＤシステム３００ａでは、コンテンツプロバイダ３０１からサービスプロバイダ３１０ａおよび３１０ｂに、同じセキュアコンテナ１０４を供給する。

【０３３５】

サービスプロバイダ３１０ａは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータＣと、当該コンテンツデータＣについて独自に作成したプライスタグデータ３１２ａとを格納したセキュアコンテナ３０４ａを作成し、これをネットワーク機器360_1に配給する。

また、サービスプロバイダ３１０ｂは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータＣと、当該コンテンツデータＣについて独自に作成したプライスタグデータ３１２ｂとを格納したセキュアコンテナ３０４ｂを作成し、これをネットワーク機器360_1に配給する。

ここで、セキュアコンテナ３０４ａ，３０４ｂのフォーマットは、図５３を用いた説明したセキュアコンテナ３０４と同じである。

【０３３６】

ネットワーク機器$360a_1$には、サービスプロバイダ３１０ａ，３１０ｂの各々に対応したＣＡモジュール３１１ａ，３１１ｂが設けられている。

ＣＡモジュール３１１ａ，３１１ｂは、自らの要求に応じたセキュアコンテナ３０４ａ，３０４ｂの配給を、それぞれサービスプロバイダ３１０ａ，３１０ｂから受ける。

【０３３７】

次に、ＣＡモジュール３１１ａ，３１１ｂは、配給されたセキュアコンテナ３０４ａ，３０４ｂに応じたＳＰ用購入履歴データ３０９ａ，３０９ｂをそれぞれ作成し、これらをそれぞれサービスプロバイダ３１０ａ，３１０ｂに送信する。

また、ＣＡモジュール３１１ａ，３１１ｂは、セキュアコンテナ３０４ａ，３０４ｂをセッション鍵データK_{SES}で復号した後に、ＳＡＭ305_1～305_4

に出力する。

【０３３８】

次に、ＳＡＭ３０５$_1$～３０５$_4$において、共通の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて、セキュアコンテナ３０４ａ，３０４ｂ内のキーファイルＫＦが復号され、共通の権利書データ１０６に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ３０８が作成される。

【０３３９】

そして、ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８が送信される。

【０３４０】

ＥＭＤサービスセンタ３０２では、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０ａ，３１０ｂの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ１５２ｃ，１５２ｓａ，１５２ｓｂを作成する。

【０３４１】

ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓａ，１５２ｓｂを送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０ａ，３１０ｂの所有者に分配される。

【０３４２】

上述したように、ＥＭＤシステム３００ｂによれば、同じコンテンツファイルＣＦをサービスプロバイダに３１０ａ，３１０ｂに供給する場合に、当該コンテンツファイルＣＦについての権利書データ１０６を配信用鍵データＫＤ$_1$～ＫＤ$_6$で暗号化してサービスプロバイダに３１０ａ，３１０ｂに供給し、サービスプロバイダに３１０ａ，３１０ｂは暗号化された権利書データ１０６をそのまま格納したセキュアコンテナ３０４ａ，３０４ｂをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のＳＡＭ３０５$_1$～３０５$_4$では

、コンテンツファイルＣＦをサービスプロバイダに３１０ａ，３１０ｂの何れから配給を受けた場合でも、共通の権利書データ１０６に基づいて権利処理を行うことができる。

【０３４３】

なお、上述した第１変形例では、２個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【０３４４】

第２実施形態の第２変形例

図８１は、第２実施形態の第２変形例に係わる複数のコンテンツプロバイダを用いたＥＭＤシステム３００ｂの構成図である。

図８１において、図４９と同一符号を付した構成要素は、第２実施形態で説明した同一符号の構成要素と同じである。

図８１に示すように、ＥＭＤシステム３００ｂでは、コンテンツプロバイダ３０１ａ，３０１ｂからサービスプロバイダ３１０に、それぞれセキュアコンテナ１０４ａ，１０４ｂが供給される。

【０３４５】

サービスプロバイダ３１０は、例えば、コンテンツプロバイダ３０１ａ，３０１ｂが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ１０４ａについてのプライスタグデータ３１２ａと、セキュアコンテナ１０４ｂについてのプライスタグデータ３１２ｂとをそれぞれ生成し、これらを格納したセキュアコンテナ３０４ｃを作成する。

図８１に示すように、セキュアコンテナ３０４ｃには、コンテンツファイルＣＦａ，ＣＦｂ、キーファイルＫＦａ，ＫＦｂ、プライスタグデータ３１２ａ，３１２ｂ、それらの各々についてのサービスプロバイダ３１０の秘密鍵データ$K_{CP,S}$による署名データが格納されている。

【０３４６】

セキュアコンテナ３０４ｃは、ユーザホームネットワーク３０３のネットワーク機器360_1のＣＡモジュール３１１で受信された後に、$SAM305_1$～305_4において処理される。

【０３４７】

ＳＡＭ３０５$_1$～３０５$_4$では、配信用鍵データＫＤａ$_1$～ＫＤａ$_3$を用いて、キーファイルＫＦａが復号され、権利書データ１０６ａに基づいて、コンテンツファイルＣＦａについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ３０８に記述される。

また、ＳＡＭ３０５$_1$～３０５$_4$において、配信用鍵データＫＤｂ$_1$～ＫＤｂ$_3$を用いて、キーファイルＫＦｂが復号され、権利書データ１０６ｂに基づいて、コンテンツファイルＣＦｂについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ３０８に記述される。

【０３４８】

そして、ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８が送信される。

【０３４９】

ＥＭＤサービスセンタ３０２では、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１ａ，３０１ｂおよびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ１５２ｃａ，１５２ｃｂ，１５２ｓを作成する。

【０３５０】

ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃａ，１５２ｃｂ，１５２ｓを送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１ａ，３０１ｂおよびサービスプロバイダ３１０の所有者に分配される。

【０３５１】

上述したように、ＥＭＤシステム３００ｂによれば、セキュアコンテナ３０４ｃ内に格納されたコンテンツファイルＣＦａ，ＣＦｂの権利書データ１０６ａ，１０６ｂは、コンテンツプロバイダ３０１ａ，３０１ｂが作成したものをそのまま用いるため、ＳＡＭ３０５$_1$～３０５$_4$内において、権利書データ１０６ａ，１０６ｂに基づいて、コンテンツファイルＣＦａ，ＣＦｂについての権利処理が

コンテンツプロバイダ３０１ａ，３０１ｂの意向に沿って確実に行われる。

【０３５２】

なお、図８１に示す第２変形例では、２個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【０３５３】

第２実施形態の第３変形例

図８２は、第２実施形態の第３変形例に係わるＥＭＤシステムの構成図である。

上述した第２実施形態では、ＥＭＤサービスセンタ３０２が決済機関９１に対して、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済を行う場合を例示したが、本発明では、例えば、図８２に示すように、ＥＭＤサービスセンタ３０２において、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１のための決済請求権データ１５２ｃと、サービスプロバイダ３１０のための決済請求権データ１５２ｓとを作成し、これらをそれぞれコンテンツプロバイダ３０１およびサービスプロバイダ３１０に送信するようにしてもよい。

この場合には、コンテンツプロバイダ３０１は、決済請求権データ１５２ｃを用いて、ペイメントゲートウェイ９０ａを介して決済機関９１ａに決済を行う。また、サービスプロバイダ３１０は、決済請求権データ１５２ｓを用いて、ペイメントゲートウェイ９０ｂを介して決済機関９１ｂに決済を行う。

【０３５４】

第２実施形態の第４変形例

図８３は、第２実施形態の第４変形例に係わるＥＭＤシステムの構成図である。

上述した第２実施形態では、例えば現行のインターネットのようにサービスプロバイダ３１０が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ３１０が課金機能を有している場合には、ＣＡモジュール３１１において、セキュアコンテナ３０４に関するサービスプロバ

イダ３１０のサービスに対しての利用履歴データ３０８ｓを作成してサービスプロバイダ３１０に送信する。

そして、サービスプロバイダ３１０は、利用履歴データ３０８ｓに基づいて、課金処理を行って決済請求権データ１５２ｓを作成し、これを用いてペイメントゲートウェイ９０ｂを介して決済機関９１ｂに決済を行う。

一方、ＳＡＭ３０$5_1$～３０$5_4$は、セキュアコンテナ３０４に関するコンテンツプロバイダ３０１の権利処理に対しての利用履歴データ３０８ｃを作成し、これをＥＭＤサービスセンタ３０２に送信する。

ＥＭＤサービスセンタ３０２は、利用履歴データ３０８ｃに基づいて、決済請求権データ１５２ｃを作成し、これをコンテンツプロバイダ３０１に送信する。

コンテンツプロバイダ３０１は、決済請求権データ１５２ｃを用いて、ペイメントゲートウェイ９０ａを介して決済機関９１ａに決済を行う。

【０３５５】

第２実施形態の第５変形例

上述した実施形態では、図４９に示すように、ＥＭＤサービスセンタ３０２のユーザ嗜好フィルタ生成部９０１において、ＳＡＭ３０$5_1$などから受信した利用履歴データ３０８に基づいて、ユーザ嗜好フィルタデータ９０３を生成する場合を例示したが、例えば、図６７に示すＳＡＭ３０$5_1$などの利用監視部１８６で生成した利用制御状態データ１６６をリアルタイムでＥＭＤサービスセンタ３０２に送信するようにして、ＳＰ用購入履歴データ３０９において、利用制御状態データ１６６に基づいてユーザ嗜好フィルタデータ９０３を生成するようにしてもよい。

【０３５６】

第２実施形態の第６変形例

コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０$5_1$～３０$5_4$は、それぞれ自らの公開鍵データ$K_{CP,P}$, $K_{SP,P}$, $K_{SAM1,P}$～$K_{SAM4,P}$の他に、自らの秘密鍵データ$K_{CP,S}$, $K_{SP,S}$, $K_{SAM1,S}$～$K_{SAM4,S}$をＥＭＤサービスセンタ３０２に登録してもよい。

このようにすることで、ＥＭＤサービスセンタ３０２は、緊急時に、国家ある

いは警察機関などからの要請に応じて、秘密鍵データ$K_{CP,S}$, $K_{SP,S}$, $K_{SAM1,S}$～$K_{SAM4,S}$を用いて、コンテンツプロバイダ３０１とサービスプロバイダ３１０との間の通信、サービスプロバイダ３１０とＳＡＭ305_1～305_4との間の通信、並びにユーザホームネットワーク３０３内でのＳＡＭ305_1～305_4相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、ＳＡＭ305_1～305_4については、出荷時に、ＥＭＤサービスセンタ３０２によって秘密鍵データ$K_{SAM1,S}$～$K_{SAM4,S}$を生成し、これをＳＡＭ305_1～305_4に格納すると共にＥＭＤサービスセンタ３０２が保持（登録）するようにしてもよい。

【０３５７】

第２実施形態の第７変形例

上述した実施形態では、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ305_1～305_4が、相互に通信を行う場合に、ＥＭＤサービスセンタ３０２から事前に公開鍵証明書データCER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAN4}を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ305_1～305_4が、相互に通信を行う場合に、ＥＭＤサービスセンタ３０２から事前に公開鍵証明書データCER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAN4}を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ305_1～305_4が、通信時に、ＥＭＤサービスセンタ３０２から公開鍵証明書データCER_{CP}, CER_{SP}, CER_{SAM1}～CER_{SAN4}を取得してもよい。

【０３５８】

図８４は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。

なお、図８４において、図４９と同じ符号を付した構成要素は、前述した同一

符号の構成要素と同じである。また、ユーザホームネットワーク３０３ａは、前述したユーザホームネットワーク３０３と同じである。ユーザホームネットワーク３０３ｂでは、ＩＥＥＥ１３９４シリアルバスであるバス１９１を介してＳＡＭ３０$５_{11}$～３０$５_{14}$を接続している。

【０３５９】

コンテンツプロバイダ３０１がサービスプロバイダ３１０の公開鍵証明書データＣＥ$Ｒ_{SP}$を取得する場合には、例えば、通信に先立ってサービスプロバイダ３１０からコンテンツプロバイダ３０１に公開鍵証明書データＣＥ$Ｒ_{SP}$を送信する場合（図８４中（３））と、コンテンツプロバイダ３０１がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥ$Ｒ_{SP}$を取り寄せる場合（図８４中（１））とがある。

【０３６０】

また、サービスプロバイダ３１０がコンテンツプロバイダ３０１の公開鍵証明書データＣＥ$Ｒ_{CP}$を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ３０１からサービスプロバイダ３１０に公開鍵証明書データＣＥ$Ｒ_{CP}$を送信する場合（図８４中（２））と、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥ$Ｒ_{CP}$を取り寄せる場合（図８４中（４））とがある。

【０３６１】

また、サービスプロバイダ３１０がＳＡＭ３０$５_{1}$～３０$５_{4}$の公開鍵証明書データＣＥ$Ｒ_{SAM1}$～ＣＥ$Ｒ_{SAM4}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０$５_{1}$～３０$５_{4}$からサービスプロバイダ３１０に公開鍵証明書データＣＥ$Ｒ_{SAM1}$～ＣＥ$Ｒ_{SAM4}$を送信する場合（図８４中（６））と、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥ$Ｒ_{SAM1}$～ＣＥ$Ｒ_{SAM4}$を取り寄せる場合（図８４中（４））とがある。

【０３６２】

また、ＳＡＭ３０$５_{1}$～３０$５_{4}$がサービスプロバイダ３１０の公開鍵証明書データＣＥ$Ｒ_{SP}$を取得する場合には、例えば、通信に先立ってサービスプロバイダ３１０からＳＡＭ３０$５_{1}$～３０$５_{4}$に公開鍵証明書データＣＥ$Ｒ_{SP}$を送信す

る場合（図８４中（５））と、ＳＡＭ３０５$_1$～３０５$_4$がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SP}$を取り寄せる場合（図８４中（７）など）とがある。

【０３６３】

また、ＳＡＭ３０５$_1$がＳＡＭ３０５$_2$の公開鍵証明書データＣＥＲ$_{SAM2}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_2$からＳＡＭ３０５$_1$に公開鍵証明書データＣＥＲ$_{SAM2}$を送信する場合（図８４中（８））と、ＳＡＭ３０５$_1$がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM2}$を取り寄せる場合（図８４中（７）など）とがある。

【０３６４】

また、ＳＡＭ３０５$_2$がＳＡＭ３０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_1$からＳＡＭ３０５$_2$に公開鍵証明書データＣＥＲ$_{SAM1}$を送信する場合（図８４中（９））と、ＳＡＭ３０５$_2$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM1}$を取り寄せる場合と、ＳＡＭ３０５$_1$が搭載されたネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM1}$を取り寄せる場合（図８４中（７），（８））とがある。

【０３６５】

また、ＳＡＭ３０５$_4$がＳＡＭ３０５$_{13}$の公開鍵証明書データＣＥＲ$_{SAM13}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_{13}$からＳＡＭ３０５$_4$に公開鍵証明書データＣＥＲ$_{SAM13}$を送信する場合（図８４中（１２））と、ＳＡＭ３０５$_4$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM13}$を取り寄せる場合（図８４中（１０））と、ユーザホームネットワーク３０３ｂ内のネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM13}$を取り寄せる場合とがある。

【０３６６】

また、ＳＡＭ３０５$_{13}$がＳＡＭ３０５$_4$の公開鍵証明書データＣＥＲ$_{SAM4}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_4$からＳＡＭ３０５$_{13}$に公開鍵証明書データＣＥＲ$_{SAM4}$を送信する場合（図８４中（１１））と、ＳＡＭ

３０５$_{13}$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM4}$を取り寄せる場合（図８４中（１３））と、ユーザホームネットワーク３０３ｂ内のネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM4}$を取り寄せる場合とがある。

【０３６７】

第２実施形態における公開鍵証明書破棄リスト（データ）の取り扱い

第２実施形態では、ＥＭＤサービスセンタ３０２において、不正行為などに用いられたコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データＣＲＬ(Certificate Revocation List)を、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$に送信する。

なお、公開鍵証明書破棄データＣＲＬは、ＥＭＤサービスセンタ３０２の他に、例えば、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$において生成してもよい。

【０３６８】

先ず、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１の公開鍵証明書データＣＥＲ$_{CP}$を無効にする場合について説明する。

図８５に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{CP}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_1$をサービスプロバイダ３１０に送信する（図８５中（１））。サービスプロバイダ３１０は、コンテンツプロバイダ３０１から入力した署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_1$を参照して公開鍵証明書データＣＥＲ$_{CP}$の有効性を判断し、有効であると判断した場合に公開鍵データＫ$_{CP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ３０１からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【０３６９】

また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データCRL_1を、サービスプロバイダ３１０の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えば$SAM305_1$に送信する（図８５中（１），（２））。$SAM305_1$は、サービスプロバイダ３１０から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ３０１の署名データを検証する際に、公開鍵証明書破棄データCRL_1を参照して公開鍵証明書データCER_{CP}の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{CP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データCRL_1を、ユーザホームネットワーク３０３内のネットワーク機器を介して$SAM305_1$に直接送信してもよい（図８５中（３））。

【０３７０】

次に、ＥＭＤサービスセンタ３０２が、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}を無効にする場合について説明する。

図８６に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データCER_{SP}を無効にすることを示す公開鍵証明書破棄データCRL_2をコンテンツプロバイダ３０１に送信する（図８６中（１））。コンテンツプロバイダ３０１は、サービスプロバイダ３１０から入力した署名データを検証する際に、公開鍵証明書破棄データCRL_2を参照して公開鍵証明書データCER_{SP}の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{SP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ３１０からのデータを無効にする。

【０３７１】

また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データCRL_2を、サービスプロバイダ３１０の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えば$SAM305_1$に送信する（図８６中（２））。$SAM305_1$は、サービスプロバイダ３１０

から入力したセキュアコンテナ内に格納されたサービスプロバイダ３１０の署名データを検証する際に、公開鍵証明書破棄データCRL_2を参照して公開鍵証明書データCER_{SP}の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{SP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ３１０内において、公開鍵証明書破棄データCRL_2の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ３１０内において、公開鍵証明書破棄データCRL_2は、サービスプロバイダ３１０の関係者による改竄な困難な領域に格納される必要がある。

なお、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データCRL_2を、ユーザホームネットワーク３０３内のネットワーク機器を介して$SAM305_1$に直接送信してもよい（図８６中（３））。

【０３７２】

次に、ＥＭＤサービスセンタ３０２が、例えば$SAM305_2$の公開鍵証明書データCER_{SAM2}を無効にする場合について説明する。

図８７に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL_3をコンテンツプロバイダ３０１に送信する（図８７中（１））。コンテンツプロバイダ３０１は、公開鍵証明書破棄データCRL_3をサービスプロバイダ３１０に送信する。サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えば$SAM305_1$に公開鍵証明書破棄データCRL_{SAM1}を送信する（図８７中（１））。$SAM305_1$は、$SAM305_2$から入力したデータに付加された$SAM305_2$の署名データを検証する際に、公開鍵証明書破棄データCRL_3を参照して公開鍵証明書データCER_{SAM2}の有効性を判断し、有効であると判断した場合に公開鍵データ$K_{SAM2,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ３１０内において、公開鍵証明書破棄データ

CRL_3 の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ３１０内において、公開鍵証明書破棄データCRL_3 は、サービスプロバイダ３１０の関係者による改竄な困難な領域に格納される必要がある。

【０３７３】

ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データCRL_3 をサービスプロバイダ３１０を介して$SAM305_1$ に送信してもよい（図８７中（１），（２））。

また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データCRL_3 を、ユーザホームネットワーク３０３内のネットワーク機器を介して$SAM305_1$ に直接送信してもよい（図８７中（３））。

【０３７４】

また、ＥＭＤサービスセンタ３０２は、例えば$SAM305_2$ の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL_3 を作成し、これを保管する。

また、ユーザホームネットワーク３０３は、バス１９１に接続されているＳＡＭのＳＡＭ登録リストＳＲＬを作成し、これをＥＭＤサービスセンタ３０２に送信する（図８８中（１））。

ＥＭＤサービスセンタ３０２は、ＳＡＭ登録リストに示される$SAM305_1$～305_4 のうち、公開鍵証明書破棄データCRL_3 によって無効にすることが示されているＳＡＭ（例えば$SAM305_2$ ）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定して新たなＳＡＭ登録リストＳＲＬを作成する。

次に、ＥＭＤサービスセンタ３０２は、当該生成したＳＡＭ登録リストＳＲＬを$SAM305_1$ に送信する（図８８中（１））。

$SAM305_1$ は、他のＳＡＭと通信を行う際に、ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０３７５】

また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を作成し、これをコンテンツプロバイダ３０１に送信する（図８８中（２））。

コンテンツプロバイダ３０１は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０に送信する（図８８中（２））。

次に、サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データＣＲＬ$_3$をＳＡＭ３０５$_1$に送信する（図８８中（２））。

ＳＡＭ３０５$_1$は、自らが作成したＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定する。

以後、ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、当該ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０３７６】

また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を作成し、これをサービスプロバイダ３１０に送信する（図８８中（３））。

次に、サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データＣＲＬ$_3$をＳＡＭ３０５$_1$に送信する（図８８中（３））。

ＳＡＭ３０５$_1$は、自らが作成したＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定する。

以後、ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、当該ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０３７７】

ＥＭＤサービスセンタ３０２の役割等

図８９は、図４９に示すＥＭＤサービスセンタ（クリアリングハウス））３０２の機能を権利管理用クリアリングハウス９５０と、電子決済用クリアリングハウス９５１とに分割した場合のＥＭＤシステムの構成図である。

当該ＥＭＤシステムでは、電子決済用クリアリングハウス９５１において、ユーザホームネットワーク３０３ａ，３０３ｂのＳＡＭからの利用履歴データ３０８に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ９０を介して決済機関９１において決済を行う。

【０３７８】

また、権利管理用クリアリングハウス９５０は、電子決済用クリアリングハウス９５１からの決済通知に応じたコンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済レポートを作成し、それらをコンテンツプロバイダ３０１およびコンテンツプロバイダ３０１に送信する。

また、コンテンツプロバイダ３０１の権利書データ１０６およびコンテンツ鍵データＫｃの登録（権威化）などを行う。

なお、図９０に示すように、権利管理用クリアリングハウス９５０と電子決済用クリアリングハウス９５１とを単体の装置内に収納すると、図４９に示すＥＭＤサービスセンタ３０２となる。

【０３７９】

また、本発明は、例えば、図９１に示すように、ＥＭＤサービスセンタ３０２に、権利管理用クリアリングハウス９６０の機能を設け、権利管理用クリアリングハウス９６０において、権利書データ１０６の登録などを行うと共に、ＳＡＭからの利用履歴データ３０８に基づいてサービスプロバイダ３１０の決済請求権データを作成し、これをサービスプロバイダ３１０に送信してもよい。この場合には、サービスプロバイダ３１０は、自らの課金システムを電子決済用クリアリングハウス９６１として利用し、権利管理用クリアリングハウス９６０からの決済請求権データに基づいて決済を行う。

【０３８０】

また、本発明は、例えば、図９２に示すように、ＥＭＤサービスセンタ３０２に、権利管理用クリアリングハウス９７０の機能を設け、権利管理用クリアリングハウス９７０において、権利書データ１０６の登録などを行うと共に、ＳＡＭからの利用履歴データ３０８に基づいてコンテンツプロバイダ３０１の決済請求権データを作成し、これをコンテンツプロバイダ３０１に送信してもよい。この場合には、コンテンツプロバイダ３０１は、自らの課金システムを電子決済用クリアリングハウス９６１として利用し、権利管理用クリアリングハウス９７０からの決済請求権データに基づいて決済を行う。

【０３８１】

第２実施形態の第８変形例

上述した第２実施形態では、図４９に示すＥＭＤシステム３００において、コンテンツプロバイダ３０１からサービスプロバイダ３１０に図４に示すフォーマットのセキュアコンテナ１０４を提供し、サービスプロバイダ３１０からユーザホームネットワーク３０３に図５３に示すフォーマットのセキュアコンテナ３０４を配給する場合を例示した。

すなわち、上述した第２実施形態では、図４および図５３に示すように、セキュアコンテナ１０４およびセキュアコンテナ３０４内に、それぞれ単数のコンテンツファイルＣＦと、当該コンテンツファイルＣＦに対応する単数のキーファイルＫＦを格納した場合を例示した。

本発明では、セキュアコンテナ１０４およびセキュアコンテナ３０４内に、それぞれ複数のコンテンツファイルＣＦと、当該複数のコンテンツファイルＣＦにそれぞれ対応する複数のキーファイルＫＦとを格納してもよい。

【０３８２】

図９３は、本変形例において、図４９に示すコンテンツプロバイダ３０１からサービスプロバイダ３１０に提供されるセキュアコンテナ１０４ａのフォーマットを説明するための図である。

図９３に示すように、セキュアコンテナ１０４ａには、コンテンツファイルCF_{101}，CF_{102}，CF_{103}、キーファイルKF_{101}，KF_{102}，KF_{103}、公

開鍵証明書データCER_{CP}、署名データ$SIG_{1,ESC}$および署名データ$SIG_{250,CP}$が格納されている。

ここで、署名データ$SIG_{250,CP}$は、コンテンツプロバイダ３０１において、コンテンツファイルCF_{101}，CF_{102}，CF_{103}、キーファイルKF_{101}，KF_{102}，KF_{103}、公開鍵証明書データCER_{CP}および署名データ$SIG_{1,ESC}$の全体に対してハッシュ値をとり、コンテンツプロバイダ３０１の秘密鍵データ$K_{cp,s}$を用いて生成される。

【０３８３】

コンテンツファイルCF_{101}には、ヘッダ、リンクデータLD_1、メタデータ$Meta_1$、コンテンツデータC_1およびＡ／Ｖ伸長用ソフトウェア$Soft_1$が格納されている。

ここで、コンテンツデータC_1およびＡ／Ｖ伸長用ソフトウェア$Soft_1$は、前述したコンテンツ鍵データKc_1を用いて暗号化されており、メタデータ$Meta_1$は必要に応じてコンテンツ鍵データKc_1を用いて暗号化されている。

また、コンテンツデータC_1は、例えば、ＡＴＲＡＣ３方式で圧縮されている。Ａ／Ｖ伸長用ソフトウェア$Soft_1$は、ＡＴＲＡＣ３方式の伸長用のソフトウェアである。

また、リンクデータLD_1は、キーファイルKF_{101}にリンクすることを示している。

【０３８４】

コンテンツファイルCF_{102}には、ヘッダ、リンクデータLD_1、メタデータ$Meta_2$、コンテンツデータC_2およびＡ／Ｖ伸長用ソフトウェア$Soft_2$が格納されている。

ここで、コンテンツデータC_2およびＡ／Ｖ伸長用ソフトウェア$Soft_2$は、前述したコンテンツ鍵データKc_2を用いて暗号化されており、メタデータ$Meta_2$は必要に応じてコンテンツ鍵データKc_2を用いて暗号化されている。

また、コンテンツデータC_2は、例えば、ＭＰＥＧ２方式で圧縮されている。Ａ／Ｖ伸長用ソフトウェア$Soft_2$は、ＭＰＥＧ２方式の伸長用のソフトウェアである。

また、リンクデータLD_2は、キーファイルKF_{102}にリンクすることを示している。

【０３８５】

コンテンツファイルCF_{103}には、ヘッダ、リンクデータLD_3、メタデータ$Meta_3$、コンテンツデータC_3およびＡ／Ｖ伸長用ソフトウェア$Soft_3$が格納されている。

ここで、コンテンツデータC_3およびＡ／Ｖ伸長用ソフトウェア$Soft_3$は、前述したコンテンツ鍵データKc_3を用いて暗号化されており、メタデータ$Meta_3$は必要に応じてコンテンツ鍵データKc_3を用いて暗号化されている。

また、コンテンツデータC_3は、例えば、ＪＰＥＧ方式で圧縮されている。Ａ／Ｖ伸長用ソフトウェア$Soft_3$は、ＪＰＥＧ方式の伸長用のソフトウェアである。

また、リンクデータLD_3は、キーファイルKF_{103}にリンクすることを示している。

【０３８６】

キーファイルKF_{101}には、ヘッダと、それぞれ配信鍵データKD_1～KD_3を用いて暗号化されたコンテンツ鍵データKc_1、権利書データ106_1、ＳＡＭプログラム・ダウンロード・コンテナSDC_1および署名・証明書モジュールMod_{200}とが格納されている。

ここで、署名・証明書モジュールMod_{200}には、図９４（Ａ）に示すように、それぞれコンテンツデータC_1，コンテンツ鍵データKc_1および権利書データ106_1のハッシュ値をとり、コンテンツプロバイダ３０１の秘密鍵データ$K_{CP,S}$を用いて作成した署名データ$SIG_{211,CP}$，$SIG_{212,CP}$，$SIG_{213,CP}$と、公開鍵データ$K_{CP,P}$の公開鍵証明書データCER_{CP}と、当該公開鍵証明書データCER_{CP}に対してのＥＭＤサービスセンタ３０２の署名データ$SIG_{1,ESC}$とが格納されている。

【０３８７】

キーファイルKF_{102}には、ヘッダと、それぞれ配信鍵データKD_1～KD_3を用いて暗号化されたコンテンツ鍵データKc_2、権利書データ106_2、ＳＡ

Ｍプログラム・ダウンロード・コンテナＳＤＣ$_2$ および署名・証明書モジュールＭｏｄ$_{201}$ とが格納されている。

ここで、署名・証明書モジュールＭｏｄ$_{201}$ には、図９４（Ｂ）に示すように、それぞれコンテンツデータＣ$_2$，コンテンツ鍵データＫｃ$_2$ および権利書データ１０６$_2$ のハッシュ値をとり、コンテンツプロバイダ３０１の秘密鍵データＫ$_{CP,S}$を用いて作成した署名データＳＩＧ$_{221,CP}$，ＳＩＧ$_{222,CP}$，ＳＩＧ$_{223,CP}$と、公開鍵証明書データＣＥＲ$_{CP}$と、当該公開鍵証明書データＣＥＲ$_{CP}$に対しての署名データＳＩＧ$_{1,ESC}$ とが格納されている。

【０３８８】

キーファイルＫＦ$_{103}$ には、ヘッダと、それぞれ配信鍵データＫＤ$_1$ ～ＫＤ$_3$ を用いて暗号化されたコンテンツ鍵データＫｃ$_3$、権利書データ１０６$_3$、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_3$ および署名・証明書モジュールＭｏｄ$_{202}$ とが格納されている。

ここで、署名・証明書モジュールＭｏｄ$_{202}$ には、図９４（Ｃ）に示すように、それぞれコンテンツデータＣ$_3$，コンテンツ鍵データＫｃ$_3$ および権利書データ１０６$_3$ のハッシュ値をとり、コンテンツプロバイダ３０１の秘密鍵データＫ$_{CP,S}$を用いて作成した署名データＳＩＧ$_{231,CP}$，ＳＩＧ$_{232,CP}$，ＳＩＧ$_{233,CP}$と、公開鍵証明書データＣＥＲ$_{CP}$と、当該公開鍵証明書データＣＥＲ$_{CP}$に対しての署名データＳＩＧ$_{1,ESC}$ とが格納されている。

【０３８９】

サービスプロバイダ３１０は、図９３に示すセキュアコンテナ１０４ａの配給を受けると、ＥＭＤサービスセンタ３０２の公開鍵データＫ$_{ESC,P}$ を用いて公開鍵証明書データＣＥＲ$_{cp}$の正当性を確認した後に、当該公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{cp,P}$を用いて、署名データＳＩＧ$_{250,CP}$の正当性を確認する。

そして、サービスプロバイダ３１０は、署名データＳＩＧ$_{250,CP}$の正当性を確認すると、図９５に示すように、セキュアコンテナ１０４ａから得たコンテンツファイルＣＦ$_{101}$，ＣＦ$_{102}$，ＣＦ$_{103}$ およびキーファイルＫＦ$_{101}$，ＫＦ$_{102}$，ＫＦ$_{103}$ と、サービスプロバイダ３１０の公開鍵証明書データＣＥＲ$_{SP}$と、署

名データＳＩＧ$_{61,ESC}$と、プライスタグデータ３１２$_1$，３１２$_2$，３１２$_3$と、署名データＳＩＧ$_{260,SP}$とを格納したセキュアコンテナ３０４ａを作成する。

ここで、プライスタグデータ３１２$_1$，３１２$_2$，３１２$_3$は、それぞれコンテンツデータＣ$_1$，Ｃ$_2$，Ｃ$_3$の販売価格を示している。

また、署名データＳＩＧ$_{260,SP}$は、コンテンツファイルＣＦ$_{101}$，ＣＦ$_{102}$，ＣＦ$_{103}$、キーファイルＫＦ$_{101}$，ＫＦ$_{102}$，ＫＦ$_{103}$、公開鍵証明書データＣＥＲ$_{SP}$と、署名データＳＩＧ$_{61,ESC}$およびプライスタグデータ３１２$_1$，３１２$_2$，３１２$_3$の全体に対してハッシュ値をとり、サービスプロバイダ３１０の秘密鍵データＫ$_{Sp,s}$を用いて生成される。

【０３９０】

サービスプロバイダ３１０は、図９５に示すセキュアコンテナ３０４ａをユーザホームネットワーク３０３に配給する。

ユーザホームネットワーク３０３では、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４ａに格納された署名データＳＩＧ$_{61,ESC}$の正当性を確認した後に、公開鍵証明書データＣＥＲ$_{sp}$に格納された公開鍵データＫ$_{SP,KP}$を用いて、署名データＳＩＧ$_{260,SP}$の正当性を確認する。

その後、ＳＡＭ３０５$_1$～３０５$_4$は、コンテンツデータＣ$_{101}$，Ｃ$_{102}$，Ｃ$_{103}$についての権利処理を、リンクデータＬＤ$_1$，ＬＤ$_2$，ＬＤ$_3$に示されるリンク状態に応じて、それぞれキーファイルＫＦ$_{101}$，ＫＦ$_{102}$，ＫＦ$_{103}$に基づいて行う。

【０３９１】

なお、上述した第８変形例では、コンテンツプロバイダ３０１において、図９３に示すように、コンテンツプロバイダ３０１において、コンテンツファイルＣＦ$_{101}$，ＣＦ$_{102}$，ＣＦ$_{103}$、キーファイルＫＦ$_{101}$，ＫＦ$_{102}$，ＫＦ$_{103}$、公開鍵証明書データＣＥＲ$_{CP}$および署名データＳＩＧ$_{1,ESC}$の全体に対しての署名データＳＩＧ$_{250,CP}$を作成する場合を例示したが、例えば、コンテンツファイルＣＦ$_{101}$，ＣＦ$_{102}$，ＣＦ$_{103}$およびキーファイルＫＦ$_{101}$，ＫＦ$_{102}$，ＫＦ$_{103}$のそれぞれについて署名データを作成し、これをセキュアコンテナ１０４ａ内に格納してもよい。

また、上述した第８変形例では、サービスプロバイダ３１０において、図９５に示すように、コンテンツファイルCF_{101}，CF_{102}，CF_{103}、キーファイルKF_{101}，KF_{102}，KF_{103}、公開鍵証明書データCER_{SP}と、署名データ$SIG_{61,ESC}$およびプライスタグデータ312_1，312_2，312_3の全体に対しての署名データ$SIG_{260,SP}$を作成する場合を例示したが、これらの各々についての署名データを作成し、これらをセキュアコンテナ３０４ａに格納するようにしてもよい。

【０３９２】

また、上述した第８変形例では、セキュアコンテナ３０４において、単数のサービスプロバイダ３１０から提供を受けた複数のコンテンツファイルCF_{101}，CF_{102}，CF_{103}を単数のセキュアコンテナ３０４ａに格納してユーザホームネットワーク３０３に配給する場合を例示したが、図８１に示すように、複数のコンテンツプロバイダ３０１ａ，３０１ｂから提供を受けた複数のコンテンツファイルＣＦを、単数のセキュアコンテナに格納してユーザホームネットワーク３０３に配給してもよい。

【０３９３】

なお、図９３に示すフォーマットは、前述した第１実施形態において、図１に示すコンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を送信する場合にも同様に適用できる。

【０３９４】

また、上述した実施形態では、ＥＭＤサービスセンタにおいて、ＳＡＭから入力した利用履歴データに基づいて決済処理を行う場合を例示したが、ＳＡＭにおいてコンテンツの購入形態が決定される度に利用制御状態データをＳＡＭからＥＭＤサービスセンタに送信し、ＥＭＤサービスセンタにおいて、受信した利用制御状態データを用いて決済処理を行ってもよい。

【０３９５】

以下、コンテンツプロバイダ１０１において作成されるコンテンツファイルＣＦおよびキーファイルＫＦなどの概念をまとめる。

コンテンツプロバイダ１０１がインターネットを用いてコンテンツを提供する

場合には、図９６に示すように、ヘッダ、コンテンツＩＤ、コンテンツ鍵データＫｃを用いた暗号化されたコンテンツデータＣおよび署名データを含むコンテンツファイルＣＦが作成される。当該コンテンツデータＣの取り扱いを示す権利書データと、コンテンツ鍵データＫｃとが、所定の信頼機関であるＥＭＤサービスセンタ１０２，３０２の配信用鍵データによって暗号化された後に、キーファイルＫＦに格納される。また、キーファイルＫＦには、ヘッダ、コンテンツＩＤ、必要に応じてメタデータ、署名データが格納される。

そして、コンテンツファイルＣＦおよびキーファイルＫＦが、コンテンツプロバイダ１０１からユーザホームネットワーク１０３，３０３に直接提供されたり、コンテンツプロバイダ１０１からサービスプロバイダ３１０を介してユーザホームネットワーク１０３，３０３に提供される。

【０３９６】

また、コンテンツプロバイダ１０１がインターネットを用いてコンテンツを提供する場合に、図９７に示すように、キーファイルＫＦ内にコンテンツ鍵データＫｃを格納しないで、所定の信頼機関であるＥＭＤサービスセンタ１０２，３０２の配信用鍵データによって暗号化したコンテンツ鍵データＫｃをＥＭＤサービスセンタ１０２，３０２からユーザホームネットワーク１０３，３０３に提供してもよい。

【０３９７】

また、コンテンツプロバイダ１０１がデジタル放送を用いてコンテンツを提供する場合に、例えば、図９８に示すように、コンテンツ鍵データＫｃを用いて暗号化したコンテンツデータＣと署名データとを、コンテンツプロバイダ１０１からユーザホームネットワーク１０３，３０３に、直接あるいはサービスプロバイダ３１０を介して提供する。この場合に、図９７に示すキーファイルＫＦに対応する鍵データブロックを、コンテンツプロバイダ１０１からユーザホームネットワーク１０３，３０３に、直接あるいはサービスプロバイダ３１０を介して提供する。

また、この場合に、例えば、図９９に示すように、所定の信頼機関であるＥＭＤサービスセンタ１０２，３０２の配信用鍵データによって暗号化したコンテン

ツ鍵データＫｃをＥＭＤサービスセンタ１０２，３０２からユーザホームネットワーク１０３，３０３に提供してもよい。

【０３９８】

【発明の効果】

以上説明したように、本発明によれば、データ提供装置の関係者の利益が適切に保護される。

また、本発明によれば、権利書データなどが不正に改竄されることを適切に回避できる。

また、本発明によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

【図面の簡単な説明】

【図１】

図１は、本発明の第１実施形態のＥＭＤシステムの全体構成図である。

【図２】

図２は、図１に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのＳＡＭとの間で送受信されるデータに関連するデータの流れを示す図である。

【図３】

図３は、図１に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとＥＭＤサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図４】

図４は、図１に示すコンテンツプロバイダからＳＡＭに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図５】

図５は、ＯＳＩレイヤ層と、本実施形態のセキュアコンテナの定義との対応関係を説明するための図である。

【図６】

図６は、ＲＯＭ型の記録媒体を説明するための図である。

【図７】

図７（Ａ）はコンテンツプロバイダからＥＭＤサービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図７（Ｂ）はＥＭＤサービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

【図８】

図８は、第１実施形態において、コンテンツプロバイダが、ＥＭＤサービスセンタに、自らの秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを要求する場合の処理のフローチャートである。

【図９】

図９は、第１実施形態において、コンテンツプロバイダがユーザホームネットワークのＳＡＭにセキュアコンテナを送信する場合の処理のフローチャートである。

【図１０】

図１０は、図１に示すＥＭＤサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図１１】

図１１は、図１に示すＥＭＤサービスセンタの機能ブロック図であり、ＳＡＭおよび図１に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図１２】

図１２は、第１実施形態において、ＥＭＤサービスセンタがコンテンツプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

【図１３】

図１３は、第１実施形態において、ＥＭＤサービスセンタがＳＡＭから、公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

【図１４】

図１４は、第１実施形態において、ＥＭＤサービスセンタがコンテンツプロバイダから権利書データおよびコンテンツ鍵データの登録要求を受けた場合の処理のフローチャートである。

【図１５】

図１５は、第１実施形態において、ＥＭＤサービスセンタが決済処理を行なう場合の処理のフローチャートである。

【図１６】

図１６は、図１に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図１７】

図１７は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図１８】

図１８は、図１６に示す外部メモリに記憶されるデータを説明するための図である。

【図１９】

図１９は、スタックメモリに記憶されるデータを説明するための図である。

【図２０】

図２０は、図１に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図２１】

図２１は、図１７に示す記憶部に記憶されるデータを説明するための図である。

【図２２】

図２２は、第１実施形態において、セキュアコンテナをコンテンツプロバイダから入力し、セキュアコンテナ内のキーファイルＫＦを復号する際のＳＡＭ内での処理のフローチャートである。

【図２３】

図２３は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図２４】

図２４は、第１実施形態において、コンテンツプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでの処理のフローチャートである。

【図２５】

図２５は、第１実施形態において、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

【図２６】

図２６は、図１６に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送元のＳＡＭ内での処理の流れを説明するための図である。

【図２７】

図２７は、図２６に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図２８】

図２８は、第１実施形態において、ネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルおよびキーファイルを、他のＡＶ機器のＳＡＭに転送する場合のＳＡＭ内での処理のフローチャートである。

【図２９】

図２９は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

【図３０】

図３０は、図２６に示す場合において、転送先のＳＡＭにおいて、入力したコ

ンテンツファイルなどを、ＲＡＭ型あるいはＲＯＭ型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図３１】

図３１は、第１実施形態において、他のＳＡＭから入力したコンテンツファイルなどを、ＲＡＭ型などの記録媒体に書き込む際のＳＡＭ内での処理のフローチャートである。

【図３２】

図３２、コンテンツの購入形態が未決定の図６に示すＲＯＭ型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、ＡＶ機器において購入形態を決定する際の処理の流れを説明するための図である。

【図３３】

図３３は、図３２に示す場合において、ＳＡＭ内でのデータの流れを示す図である。

【図３４】

図３４は、第１実施形態において、コンテンツの購入形態が未決定の図５に示すＲＯＭ型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、ＡＶ機器において購入形態を決定する際の処理のフローチャートである。

【図３５】

図３５は、図３４のフローチャートの続きのフローチャートである。

【図３６】

図３６は、ユーザホームネットワーク内のＡＶ機器において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナを読み出して、これを他のＡＶ機器に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図３７】

図３７は、図３６に示すように、第１のＡＶ機器において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナを読み出して第２のＡＶ機器に転送し、第２のＡＶ機器において購入形態を決定してＲＡＭ型の記録媒体に書き込む際

の第１のＡＶ機器の処理のフローチャートである。

【図３８】

図３８は、図３７に示す場合の第２のＡＶ機器の処理のフローチャートである。

【図３９】

図３９は、図３８に示すフローチャートの続きのフローチャートである。

【図４０】

図４０は、図３６に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図４１】

図４１は、図３６に示す場合における転送先のＳＡＭ内でのデータの流れを示す図である。

【図４２】

図４２は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図４３】

図４３は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図４４】

図４４は、バスへの機器の接続形態の一例を説明するための図である。

【図４５】

図４５は、ＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図４６】

図４６は、図１に示すコンテンツプロバイダの全体動作のフローチャートである。

【図４７】

図４７は、本発明の第１実施形態の第２変形例を説明するための図である。

【図４８】

図４８は、本発明の第１実施形態の第３変形例を説明するための図である。

【図４９】

図４９は、本発明の第２実施形態のＥＭＤシステムの全体構成図である。

【図５０】

図５０は、図４９に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図である。

【図５１】

図５１は、図４９に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図５２】

図５２は、第２実施形態において、コンテンツプロバイダから供給を受けたセキュアコンテナからセキュアコンテナを作成し、これをユーザホームネットワークに配給する際のサービスプロバイダの処理のフローチャートである。

【図５３】

図５３は、図４９に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図５４】

図５４は、図４９に示すサービスプロバイダの機能ブロック図であり、ＥＭＤサービスセンタとの間で送受信されるデータの流れを示す図である。

【図５５】

図５５は、サービスプロバイダからＥＭＤサービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図５６】

図５６は、図４９に示すＥＭＤサービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図で

ある。

【図５７】

図５７は、図４９に示すＥＭＤサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図５８】

図５８は、図４９に示すＥＭＤサービスセンタの機能ブロック図であり、ＳＡＭとの間で送受信されるデータに関連するデータの流れを示す図である。

【図５９】

図５９は、利用履歴データの内容を説明するための図である。

【図６０】

図６０は、第２実施形態において、ＥＭＤサービスセンタがサービスプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

【図６１】

図６１は、第２実施形態において、ＥＭＤサービスセンタが、サービスプロバイダからプライスタグデータの登録要求を受けた場合の処理のフローチャートである。

【図６２】

図６２は、第２実施形態において、ＥＭＤサービスセンタが決済を行なう場合の処理のフローチャートである。

【図６３】

図６３は、図４９に示すネットワーク機器の構成図である。

【図６４】

図６４は、図６３に示すＣＡモジュールの機能ブロック図である。

【図６５】

図６５は、図６３に示すＳＡＭの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図６６】

図６６は、図６５に示す記憶部に記憶されるデータを説明するための図である。

【図６７】

図６７は、図６３に示すＳＡＭの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図６８】

図６８は、第２実施形態において、セキュアコンテナをサービスプロバイダから入力し、セキュアコンテナ内のキーファイルを復号する際のＳＡＭの処理のフローチャートである。

【図６９】

図６９は、第２実施形態において、サービスプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでのＳＡＭの処理のフローチャートである。

【図７０】

図７０は、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

【図７１】

図７１は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図７２】

図７２は、図６３に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送先のＳＡＭ内での処理の流れを説明するための図である。

【図７３】

図４９は、図７２に示す場合の転送元のＳＡＭ内でのデータの流れを示す図である。

【図７４】

図７４は、図７２に示すように、例えば、ネットワーク機器のダウンロードメ

モリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送元のＳＡＭの処理のフローチャートである。

【図７５】

図７５は、ネットワーク機器のＳＡＭからＡＶ機器のＳＡＭに転送される購入形態が既に決定されたセキュアコンテナのフォーマットを説明するための図である。

【図７６】

図５１は、図７２に示す場合の転送先のＳＡＭ内でのデータの流れを示す図である。

【図７７】

図７７は、図７２に示すように、他のＳＡＭから入力したコンテンツファイルなどを、ＲＡＭ型などの記録媒体に書き込む際のＳＡＭの処理のフローチャートである。

【図７８】

図７８は、図４９に示すＥＭＤシステムの全体動作のフローチャートである。

【図７９】

図７９は、図４９に示すＥＭＤシステムの全体動作のフローチャートである。

【図８０】

図８０は、本発明の第２実施形態の第１変形例に係わる２個のサービスプロバイダを用いたＥＭＤシステムの構成図である。

【図８１】

図８１は、本発明の第２実施形態の第２変形例に係わる複数のコンテンツプロバイダを用いたＥＭＤシステムの構成図である。

【図８２】

図８２は、本発明の第２実施形態の第３変形例に係わるＥＭＤシステムの構成図である。

【図８３】

図８３は、本発明の第２実施形態の第４変形例に係わるＥＭＤシステムの構成

図である。

【図８４】

図８４は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図８５】

図８５は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図８６】

図８６は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図８７】

図８７は、ＳＡＭの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図８８】

図８８は、ＳＡＭの公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図８９】

図８９は、図４９に示すＥＭＤシステムにおいて、ＥＭＤサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図９０】

図９０は、図８９に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のＥＭＤサービスセンタ内に設けた場合のＥＭＤシステムの構成図である。

【図９１】

図９１は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のＥＭＤシステムの構成図である。

【図９２】

図９２は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に

決済を行う場合のＥＭＤシステムの構成図である。

【図９３】

図９３は、本発明の第２実施形態の第８変形例において、図４９に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテナのフォーマットを説明するための図である。

【図９４】

図９４は、図９３に格納されたモジュールの詳細なフォーマットを説明するための図である。

【図９５】

図９５は、本発明の第２実施形態の第８変形例において、図４９に示すサービスプロバイダからＳＡＭに提供されるセキュアコンテナのフォーマットを説明するための図である。

【図９６】

図９６は、インターネットを用いてセキュアコンテナを提供する場合の概念図である。

【図９７】

図９７は、インターネットを用いてセキュアコンテナを提供する場合のその他の概念図である。

【図９８】

図９８は、デジタル放送を用いてセキュアコンテナを提供する場合の概念図である。

【図９９】

図９９は、デジタル放送を用いてセキュアコンテナを提供する場合のその他の概念図である。

【図１００】

図１００は、従来のＥＭＤシステムの構成図である。

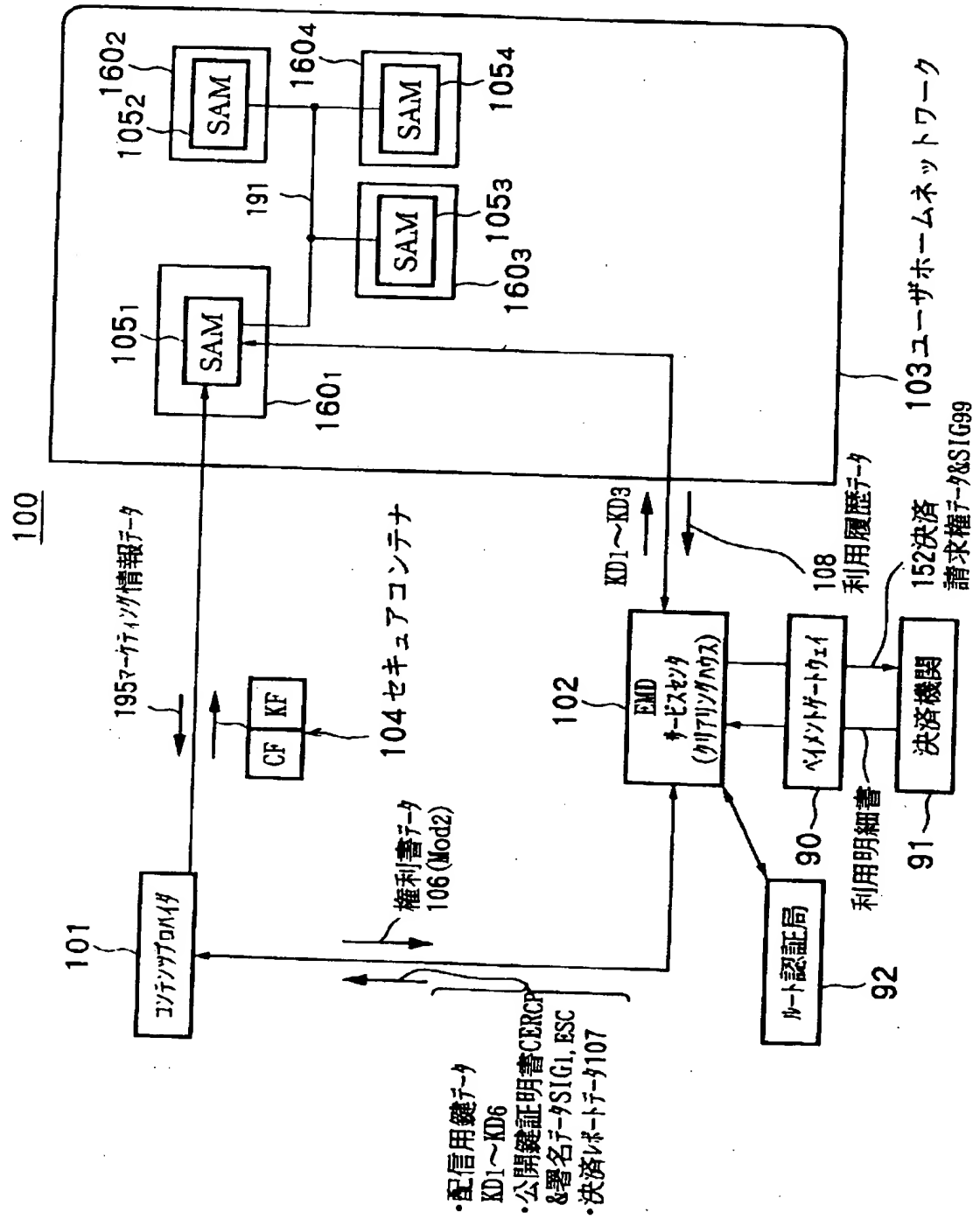
【符号の説明】

９０…ペイメントゲートウェイ、９１…決済機関、９２…ルート認証局、１００，３００…ＥＭＤシステム、１０１，３０１…コンテンツプロバイダ、１０２

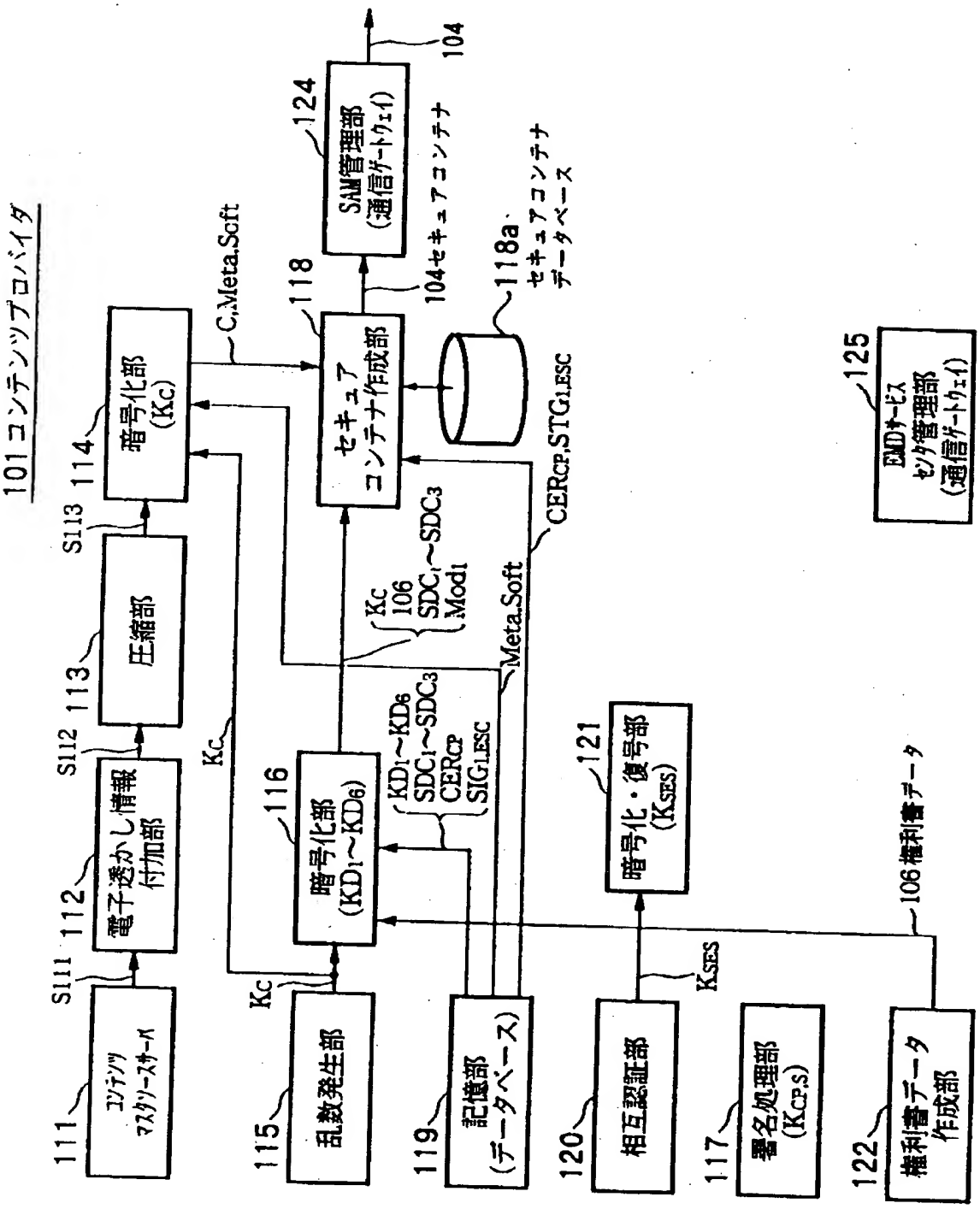
，３０２…ＥＭＤサービスセンタ、１０３，３０３…ユーザホームネットワーク、１０４，３０４…セキュアコンテナ、105_1～105_4，305_1～305_4…ＳＡＭ、１０６…権利書データ、１０７，３０７…決済レポートデータ、１０８，３０８…利用履歴データ、160_1…ネットワーク機器、160_2～160_4…ＡＶ機器、１５２，１５２ｃ，１５２ｓ…決済請求権データ、１９１…バス、３１０…サービスプロバイダ、３１１…ＣＡモジュール、３１２…プライスタグデータ、ＣＦ…コンテンツファイル、ＫＦ…キーファイル、Ｋｃ…コンテンツ鍵データ

【書類名】　図面

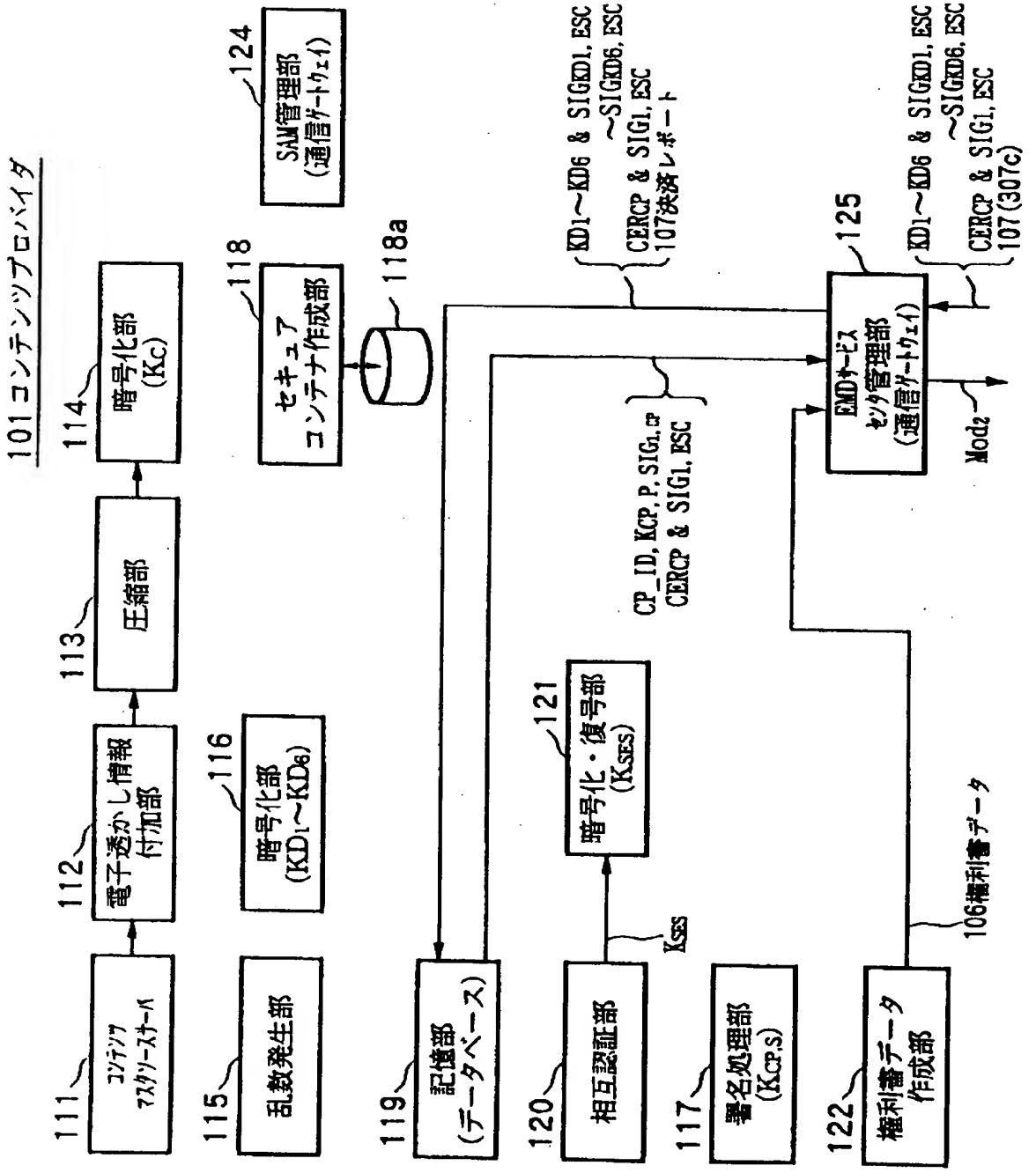
【図１】


100
SAM
1052
1602
1054
1604
1053
1603
191
1051
1601
103ユーザホームネットワーク
195マーケティング情報データ
104セキュアコンテナ
CF
KF
KD1～KD3
108
利用履歴データ
152決済
請求権データ&SIG99
102
EMD
サービスセンタ
(クリアリングハウス)
ペイメントゲートウェイ
決済機関
権利書データ
106(Mod2)
101
コンテンツプロバイダ
90
91
利用明細書
ルート認証局
92
・配信用鍵データ
KD1～KD6
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107

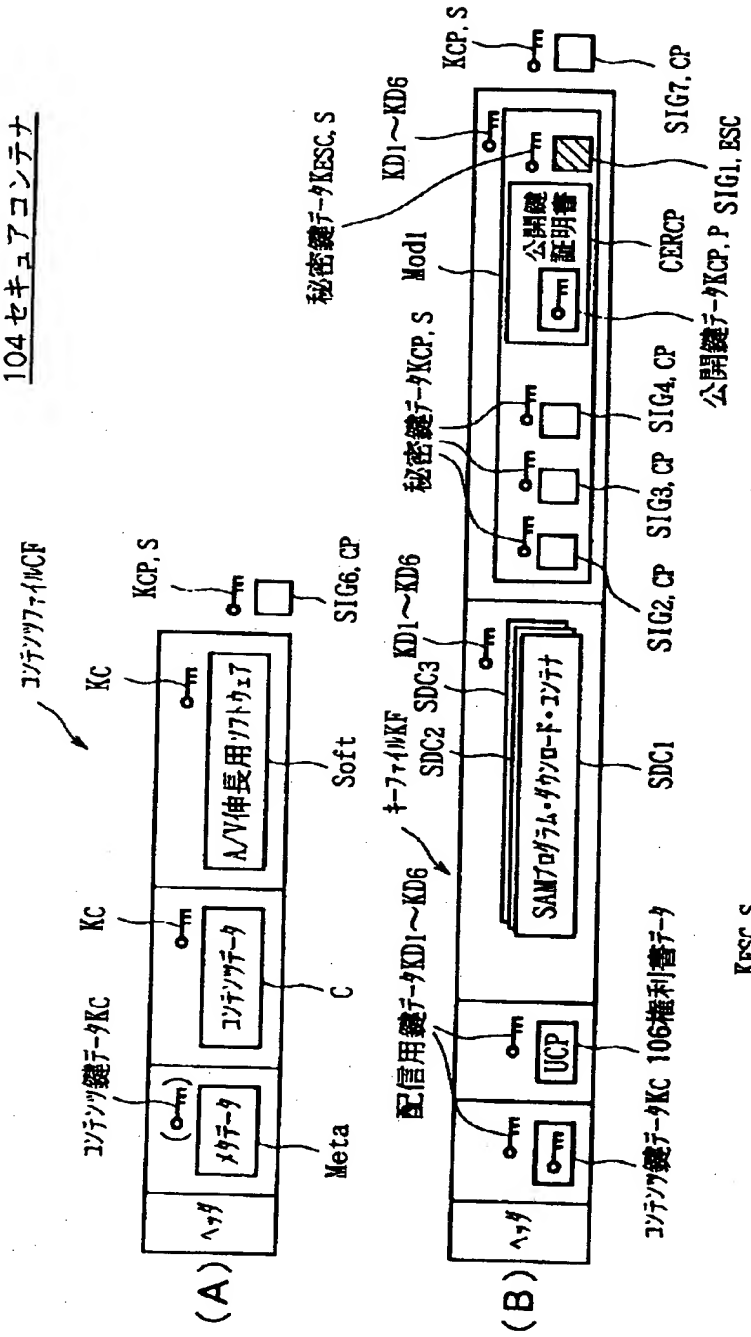
【図２】


101コンテンツプロバイダ
111 コンテンツマスタソースオーバ
112 電子透かし情報付加部
113 圧縮部
114 暗号化部 (Kc)
115 乱数発生部
116 暗号化部 (KD1～KD6)
117 署名処理部 (KCP,S)
118 セキュアコンテナ作成部
119 記憶部 (データベース)
120 相互認証部
121 暗号化・復号部 (KSES)
122 権利書データ作成部
124 SAM管理部 (通信ゲートウェイ)
125 EMDサービスセンタ管理部 (通信ゲートウェイ)
104 104セキュアコンテナ
118a セキュアコンテナデータベース
S111
S112
S113
Kc
C,Meta,Soft
Kc 106 SDC1～SDC3 Mod1
KD1～KD6 SDC1～SDC3 CERCP SIG1,ESC
Meta,Soft
CERCP,STG1,ESC
106 権利書データ
KSES

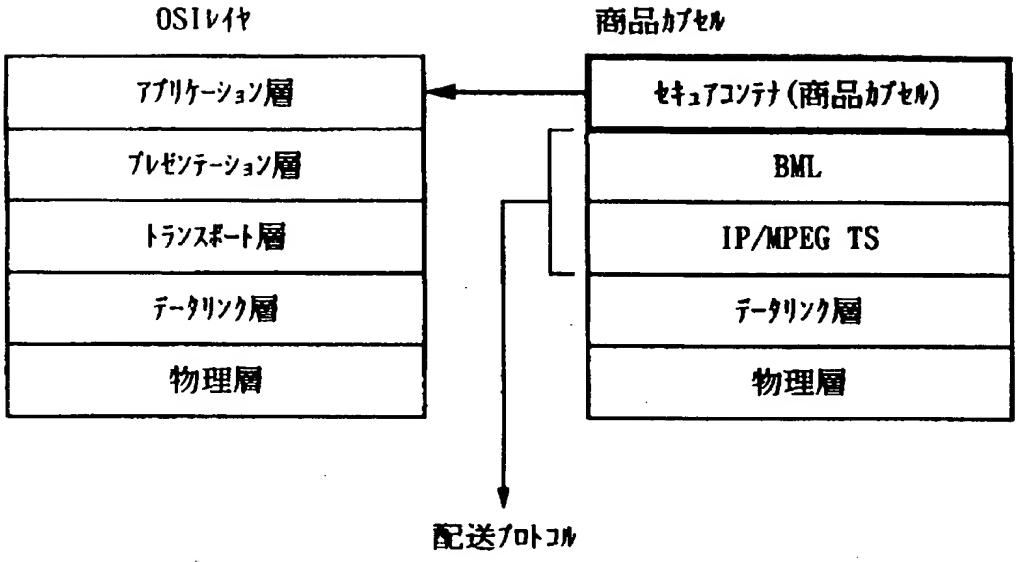
【図３】


101コンテンツプロバイダ
111 コンテンツマスターストーバ
112 電子透かし情報付加部
113 圧縮部
114 暗号化部 (Kc)
115 乱数発生部
116 暗号化部 (KD1～KD6)
118 セキュアコンテナ作成部
118a
119 記憶部 (データベース)
120 相互認証部
121 暗号化・復号部 (KSES)
117 署名処理部 (KCP,S)
122 権利書データ作成部
124 SAM管理部 (通信ゲートウェイ)
125 EMDサービスセンタ管理部 (通信ゲートウェイ)
KD1～KD6 & SIGD1, ESC ～SIGD6, ESC
CERCP & SIG1, ESC
107決済レポート
CP_ID, KCP, P, SIG1, CERCP & SIG1, ESC
KSES
106権利書データ
Mod2

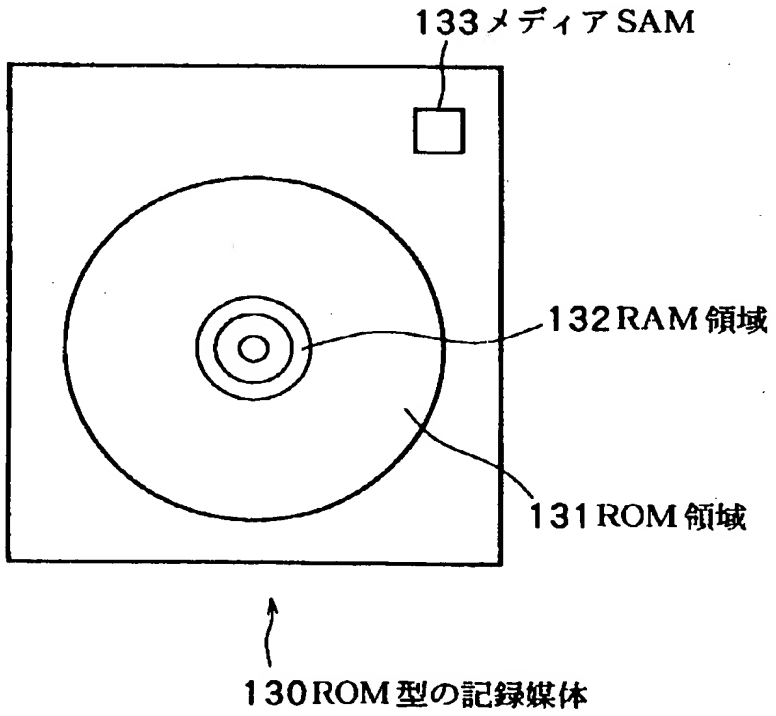
【図４】


104 セキュアコンテナ
コンテンツファイルWCF
Kc
KCP, S
SIG6, CP
ヘッダ
コンテンツ鍵データKc
メタデータ
Meta
コンテンツデータ
C
A/V伸長用ソフトウェア
Soft
(A)
秘密鍵データKESC, S
KD1～KD6
KCP, S
SIG7, CP
Mod1
公開鍵証明書
CERCP
公開鍵データKCP, P
SIG1, ESC
秘密鍵データKCP, S
SIG4, CP
SIG3, CP
SIG2, CP
KD1～KD6
SDC3
SDC2
SDC1
キーファイルWKF
配信用鍵データKD1～KD6
SAMプログラム・ダウンロード・コンテナ
UCP
106権利書データ
コンテンツ鍵データKc
(B)
KESC, S
SIG1, ESC署名データ
公開鍵証明書
CERCP
KCP, P
(C)

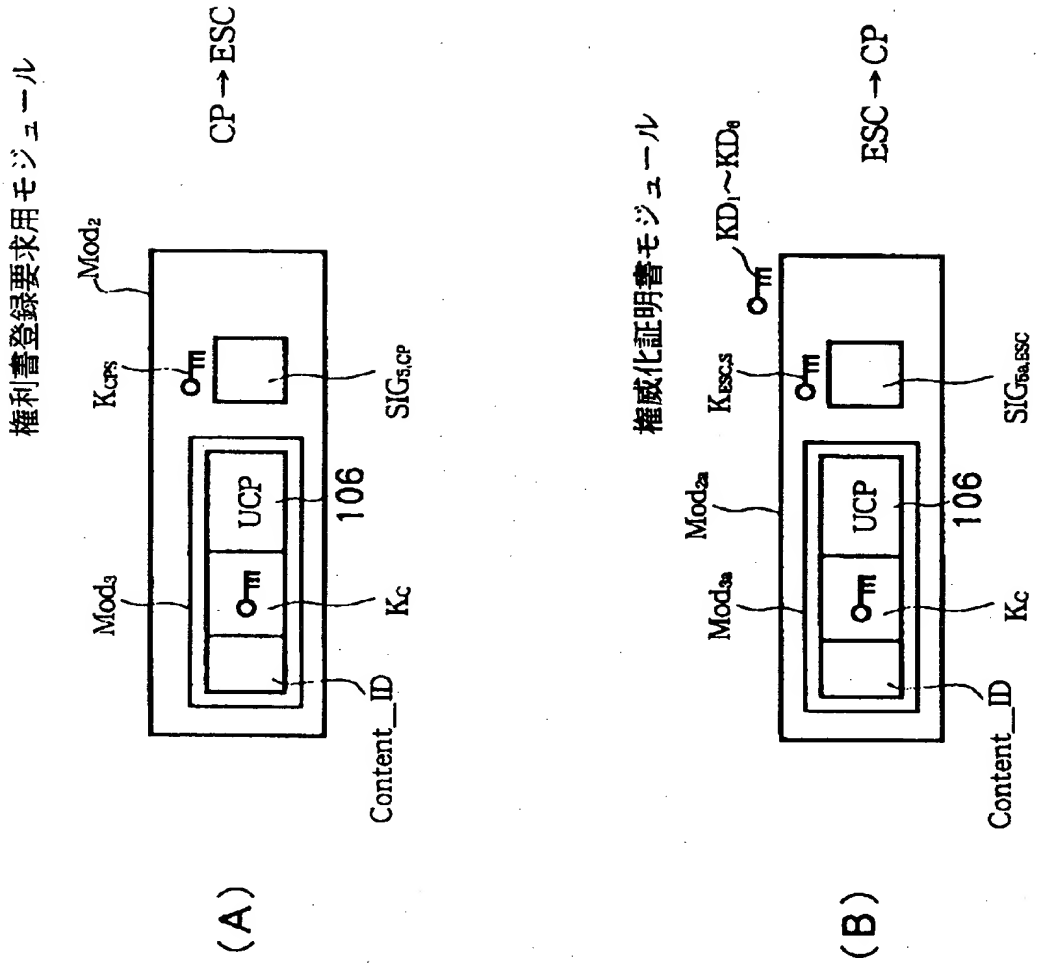
【図５】


OSIレイヤ
商品カプセル
アプリケーション層
プレゼンテーション層
トランスポート層
データリンク層
物理層
セキュアコンテナ(商品カプセル)
BML
IP/MPEG TS
データリンク層
物理層
配送プロトコル

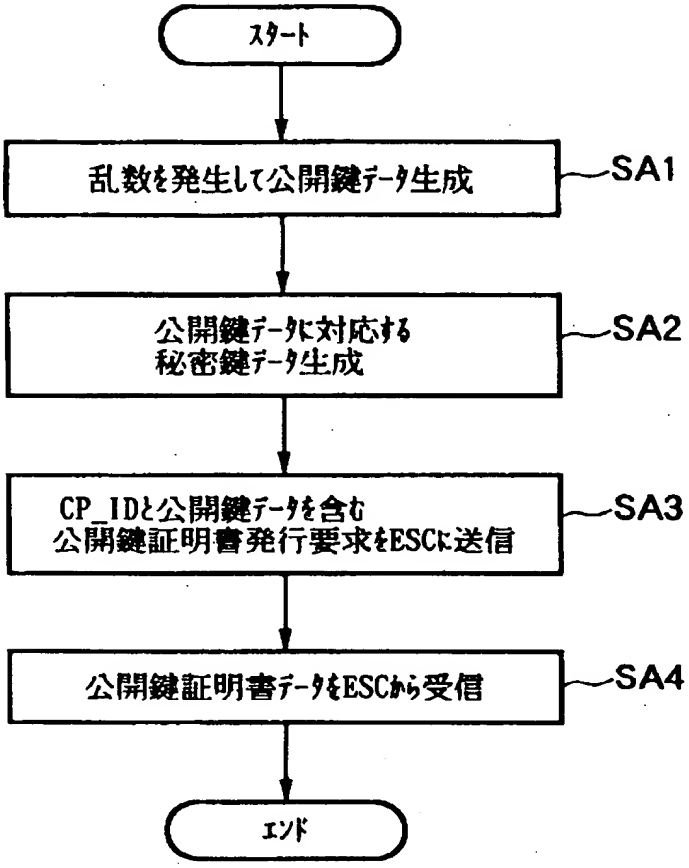
【図６】


133メディアSAM
132RAM領域
131ROM領域
130ROM型の記録媒体

【図７】

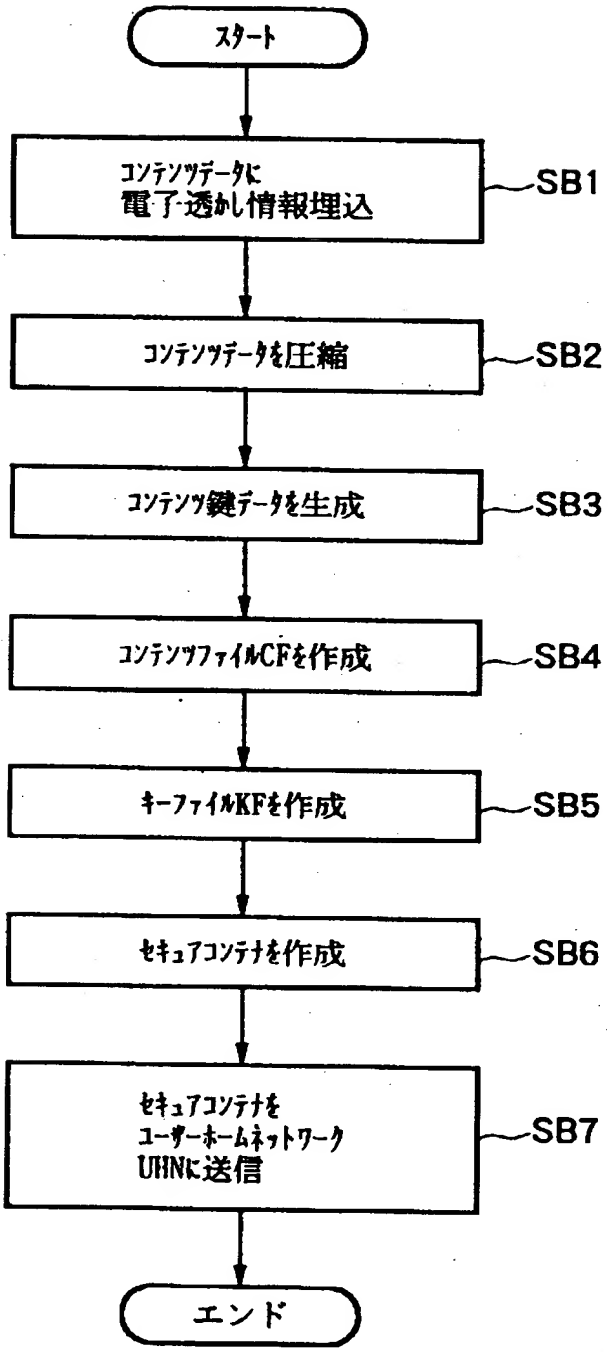

権利書登録要求用モジュール
CP→ESC
Mod2
Kcps
SIG5,CP
UCP
106
Mod3
Kc
Content_ID
(A)
権威化証明書モジュール
ESC→CP
KD1～KDn
Kesc,s
SIG6a,ESC
Mod2a
Mod3a
UCP
106
Kc
Content_ID
(B)

【図８】



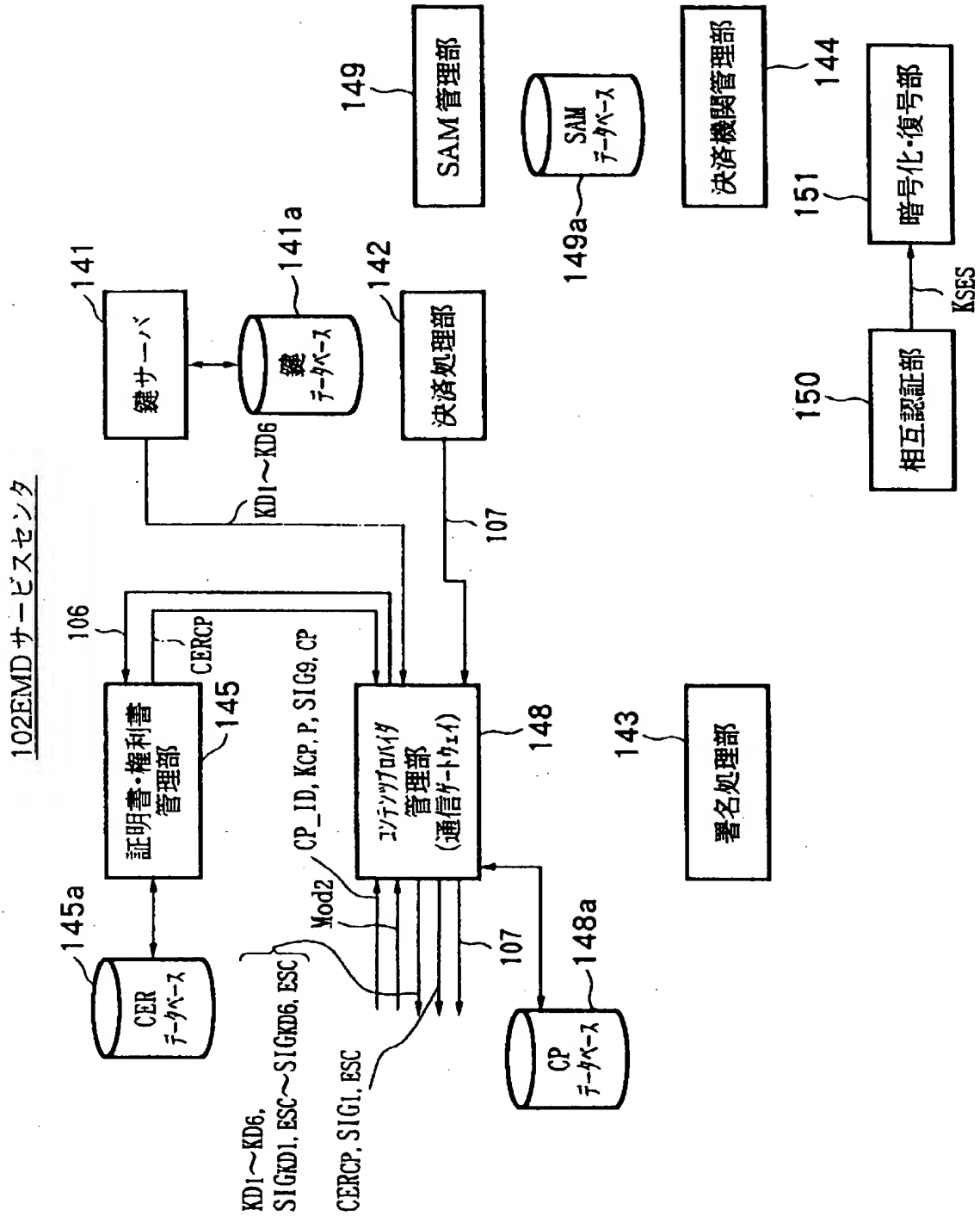
CPからESCへの公開鍵証明書データの発行要求処理

【図９】

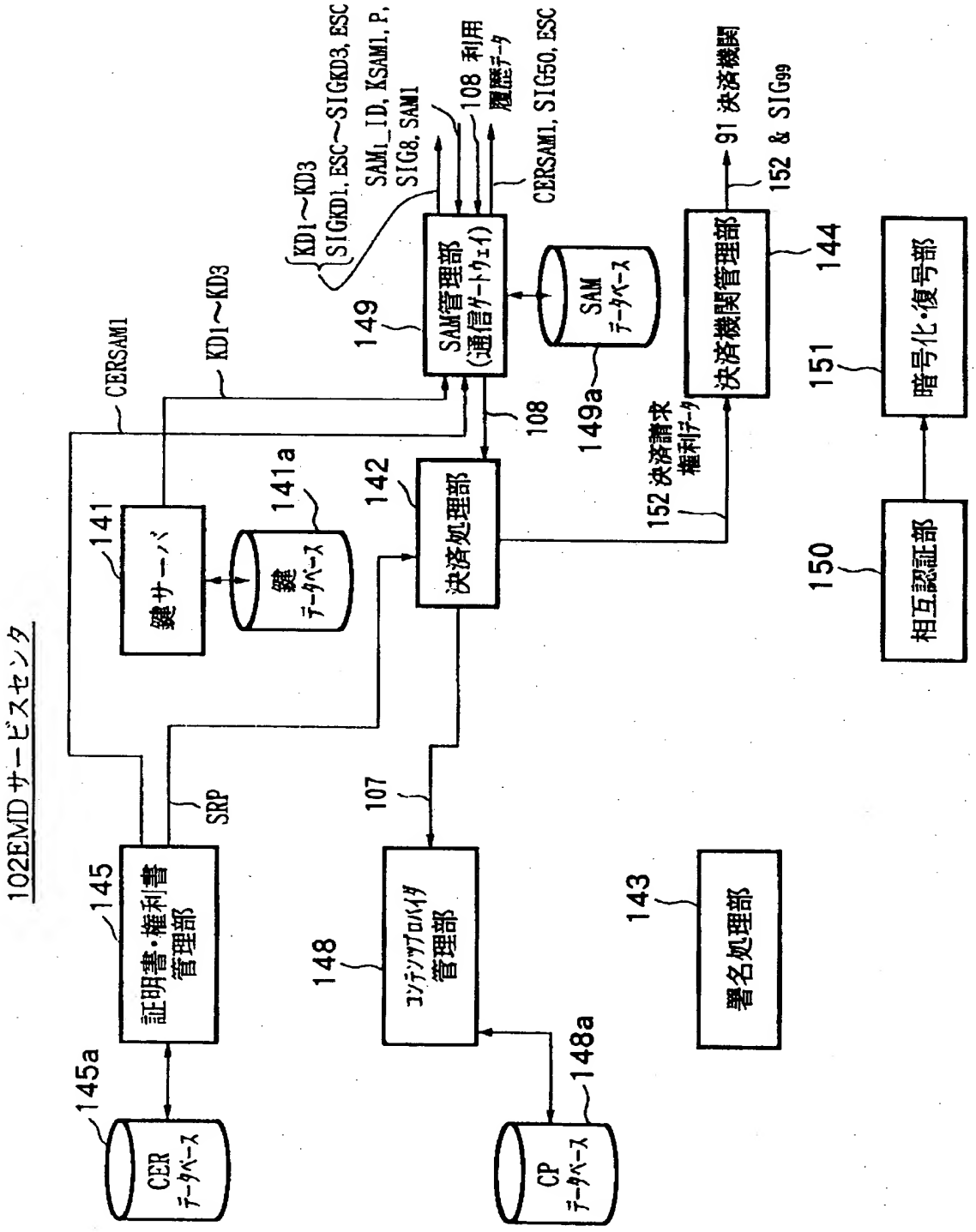


CPのセキュアコンテナ作成処理

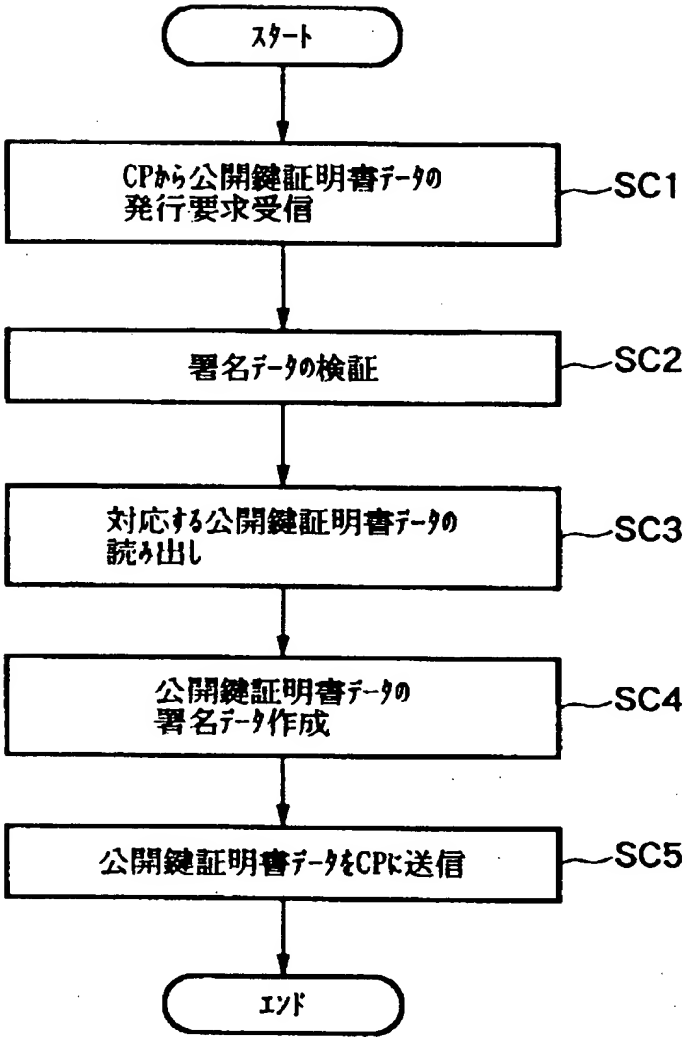
【図１０】


102EMDサービスセンタ
鍵サーバ
141
鍵データベース
141a
KD1～KD6
SAM管理部
149
SAMデータベース
149a
決済処理部
142
決済機関管理部
144
暗号化・復号部
151
KSES
相互認証部
150
107
106
CERCP
証明書・権利書管理部
145
CERデータベース
145a
CP_ID, KCP, P, SIG9, CP
Mod2
コンテンツプロバイダ管理部（通信ゲートウェイ）
148
署名処理部
143
CPデータベース
148a
KD1～KD6,
SIGKD1, ESC～SIGKD6, ESC
CERCP, SIG1, ESC

【図１１】

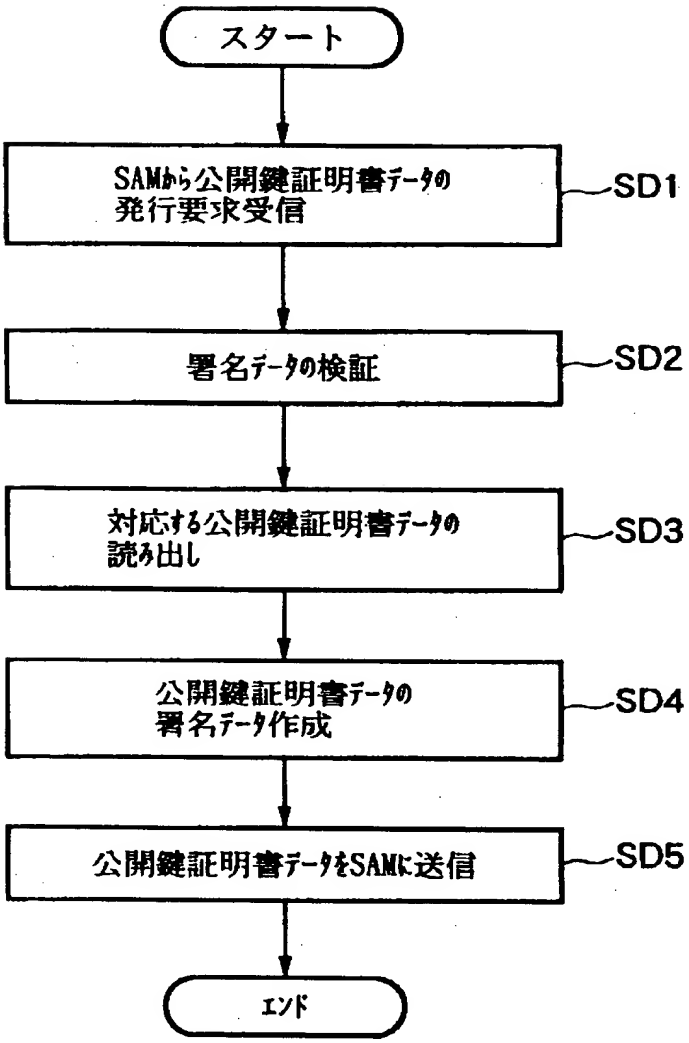

102EMDサービスセンタ
CERSAM1
KD1～KD3
KD1～KD3
SIGKD1, ESC～SIGKD3, ESC
SAM1_ID, KSAM1, P,
SIG8, SAM1
108 利用
履歴データ
CERSAM1, SIG50, ESC
91 決済機関
152 & SIG99
149
SAM管理部
(通信ゲートウェイ)
SAM
データベース
決済機関管理部
144
151
暗号化・復号部
108
149a
152 決済請求
権利データ
141
鍵サーバ
141a
鍵
データベース
142
決済処理部
150
相互認証部
145
証明書・権利書
管理部
SRP
107
148
コンテンツプロバイダ
管理部
143
署名処理部
145a
CER
データベース
148a
CP
データベース

【図１２】



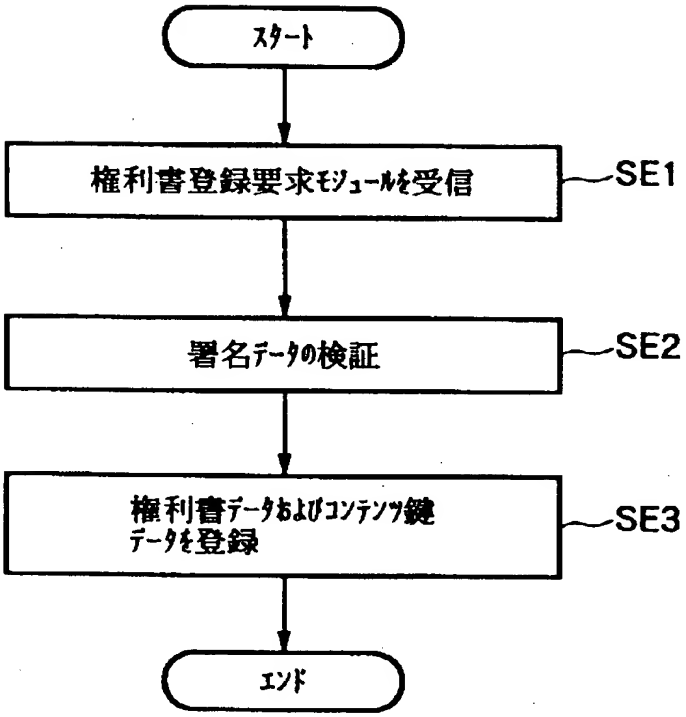
CPからの公開鍵証明書データの発行要求に応じたESCの処理

【図１３】



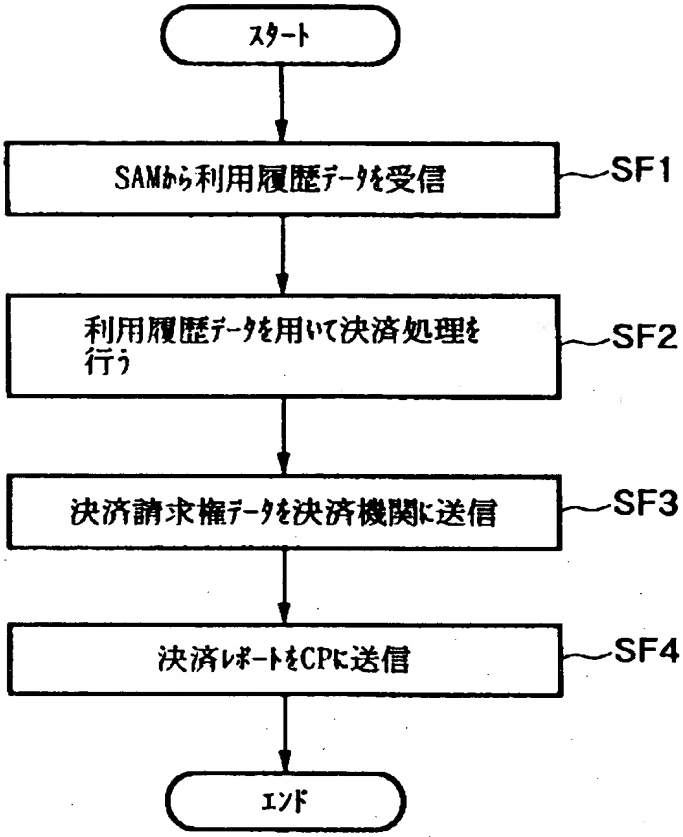
SAMからの公開鍵証明書データの発行要求に応じたESCの処理

【図１４】



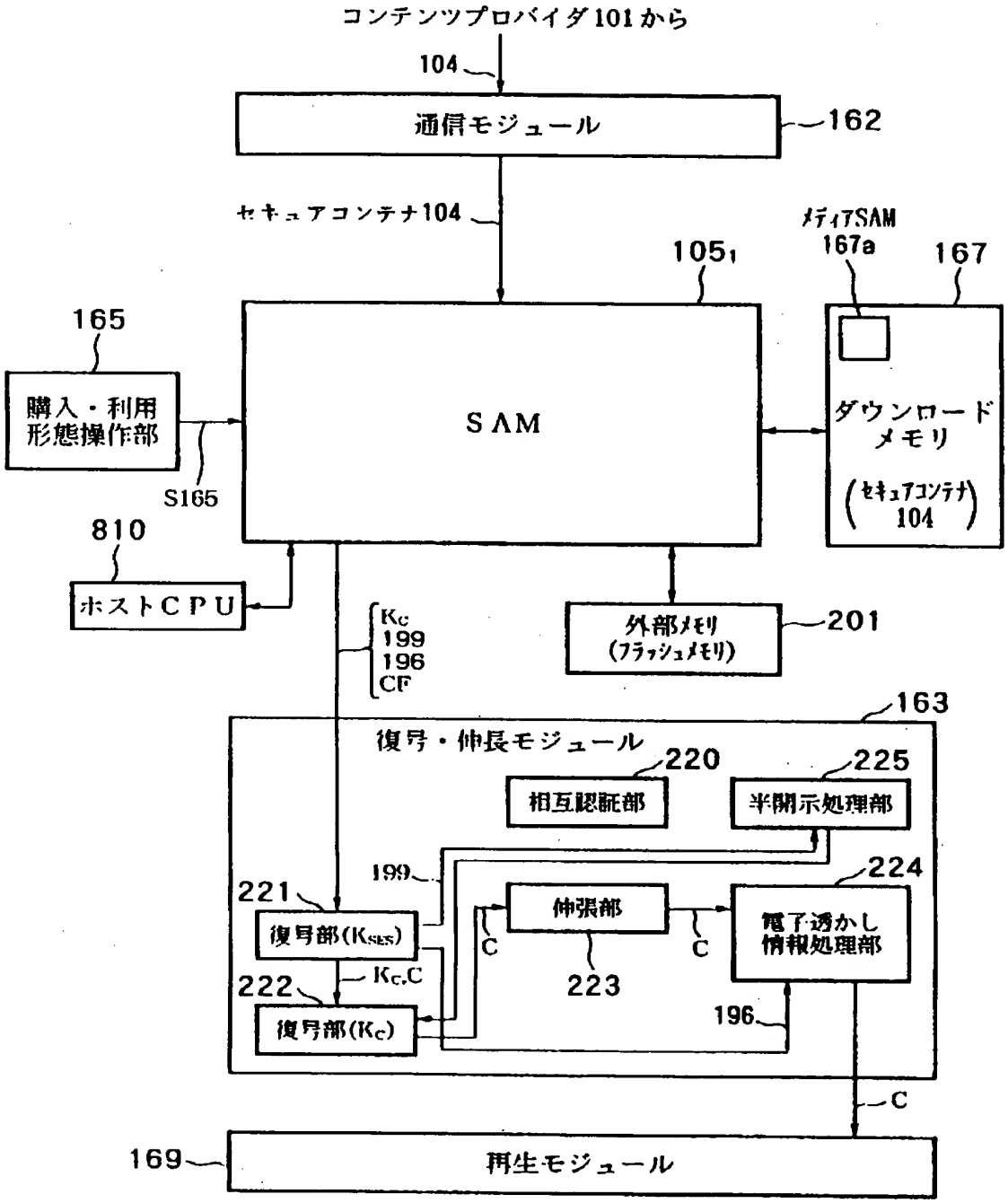
ESCにおける権利書データおよびコンテンツ鍵データの登録処理

【図１５】

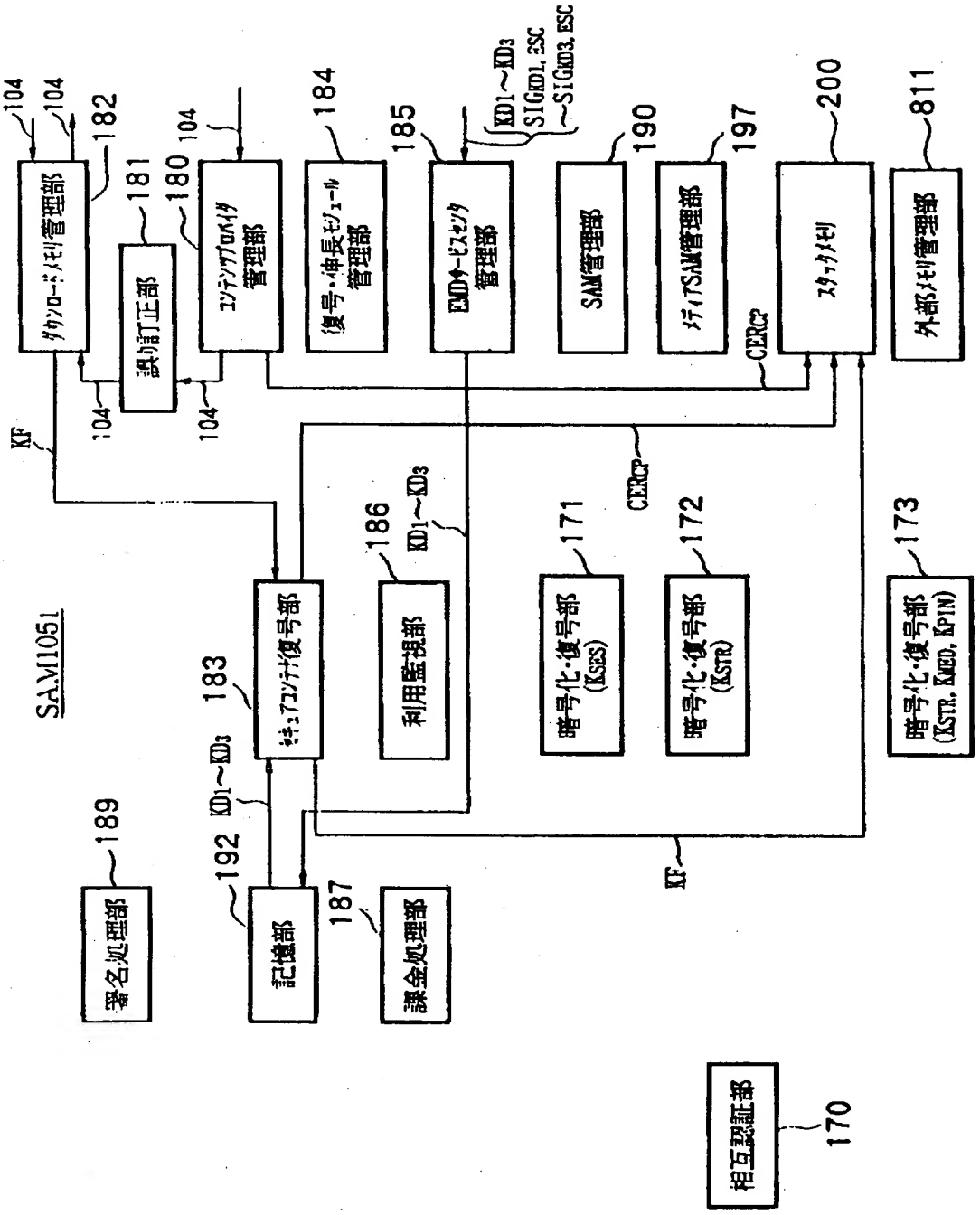


ESCにおける決済処理

【図１６】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
メディアSAM
167a
167
105₁
165
購入・利用
形態操作部
SAM
ダウンロード
メモリ
(セキュアコンテナ
104)
S165
810
ホストCPU
Kc
199
196
CF
外部メモリ
(フラッシュメモリ)
201
163
復号・伸長モジュール
220
相互認証部
225
半開示処理部
199
224
221
伸張部
電子透かし
情報処理部
復号部(KSES)
C
C
223
Kc.C
222
196
復号部(Kc)
C
169
再生モジュール

【図１７】


104
104
182
181
180
104
184
185
KD1～KD3
SIGCD1, ESC
～SIGCD3, ESC
190
197
200
811
CERCP
KF
104
104
186
KD1～KD3
171
172
173
CERCP
SAM105
183
KD1～KD3
189
192
187
KF
170

【図１８】

外部メモリ201に記憶されるデータ

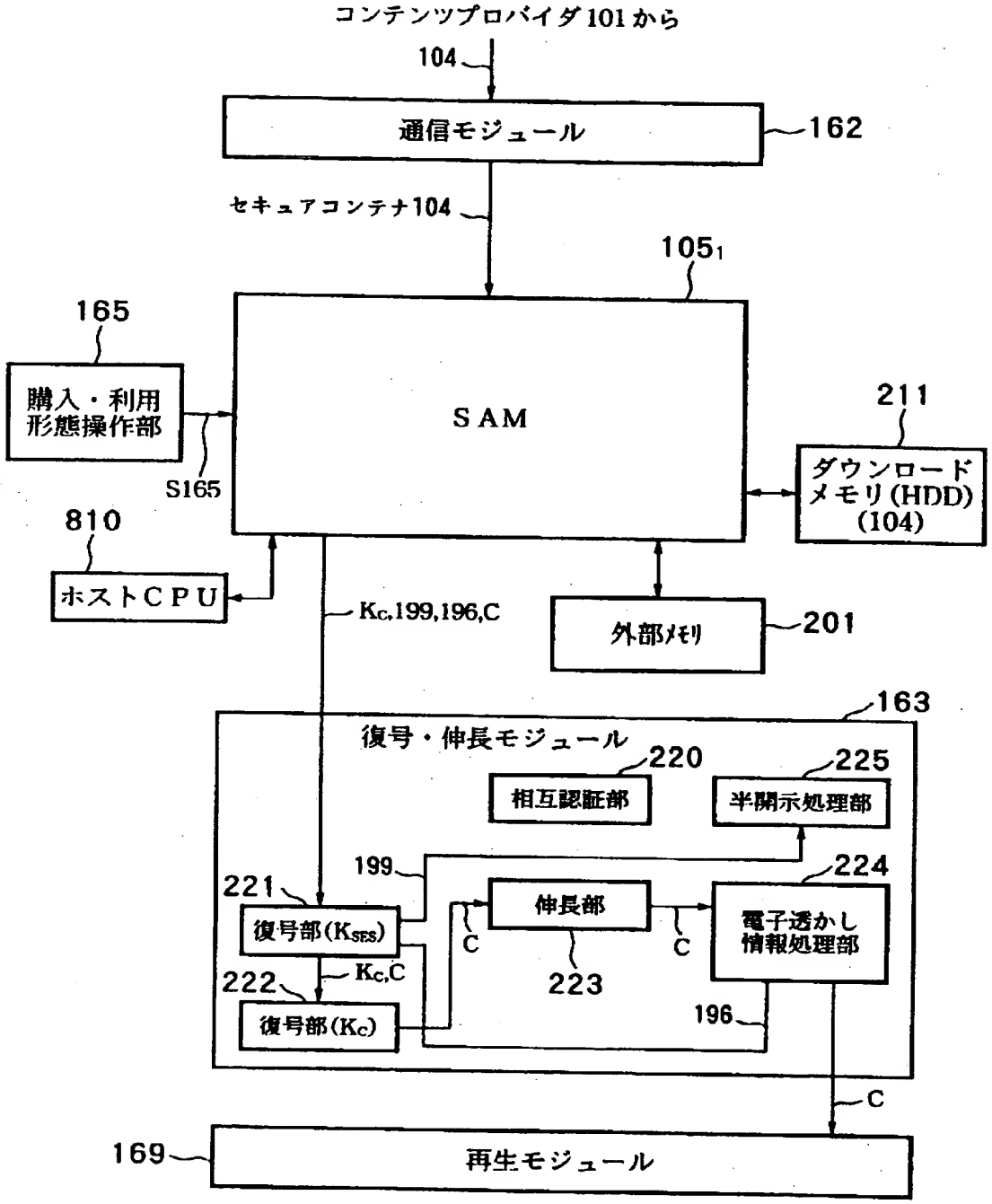
利用履歴データ108
SAM登録リスト

【図１９】

スタックメモリ200に記憶されるデータ

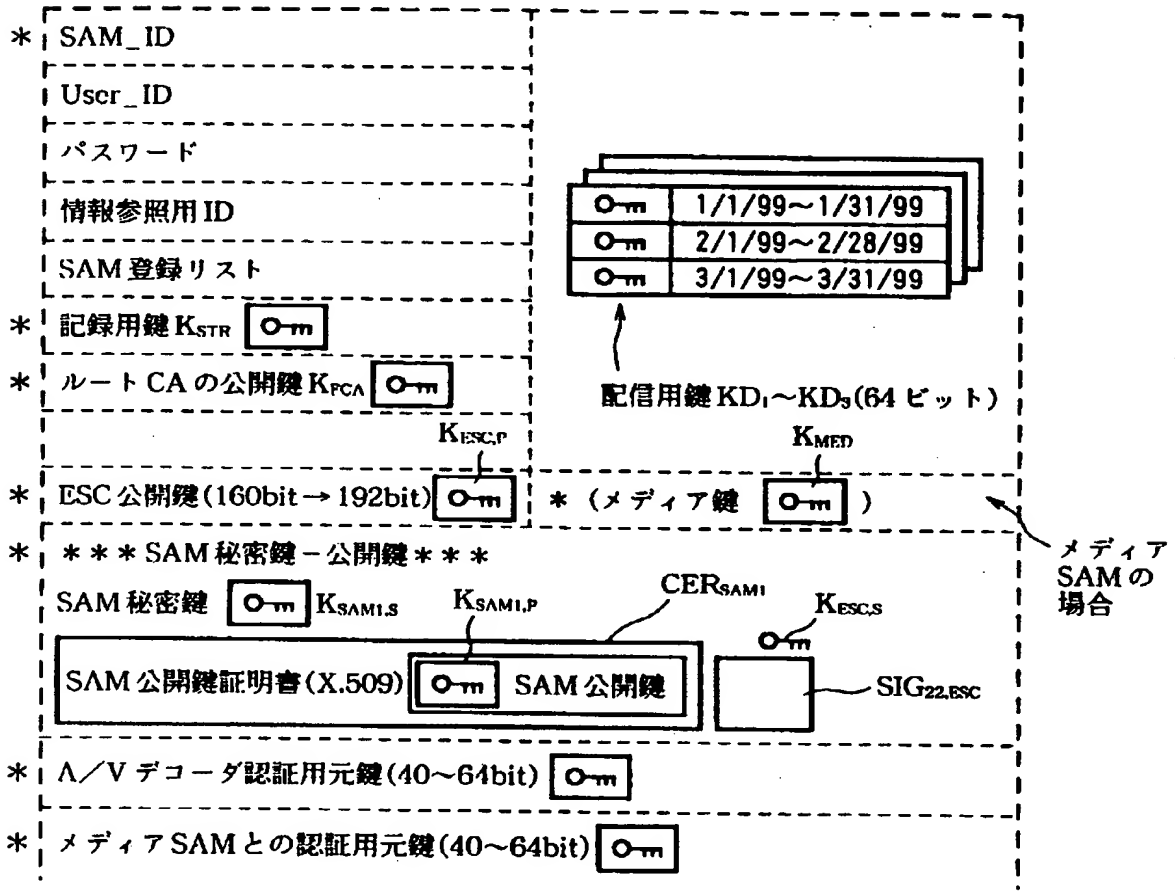
コンテンツ鍵データKc
権利書データ（UCP）106
記憶部（フラッシュメモリ）192のロック鍵データK_{LOC}
コンテンツプロバイダ101の公開鍵証明書CER_{CP}
利用制御情状態データ（UCS）166
SAMプログラム・ダウンロード・コンテナSD_1～SDC_3

【図２０】

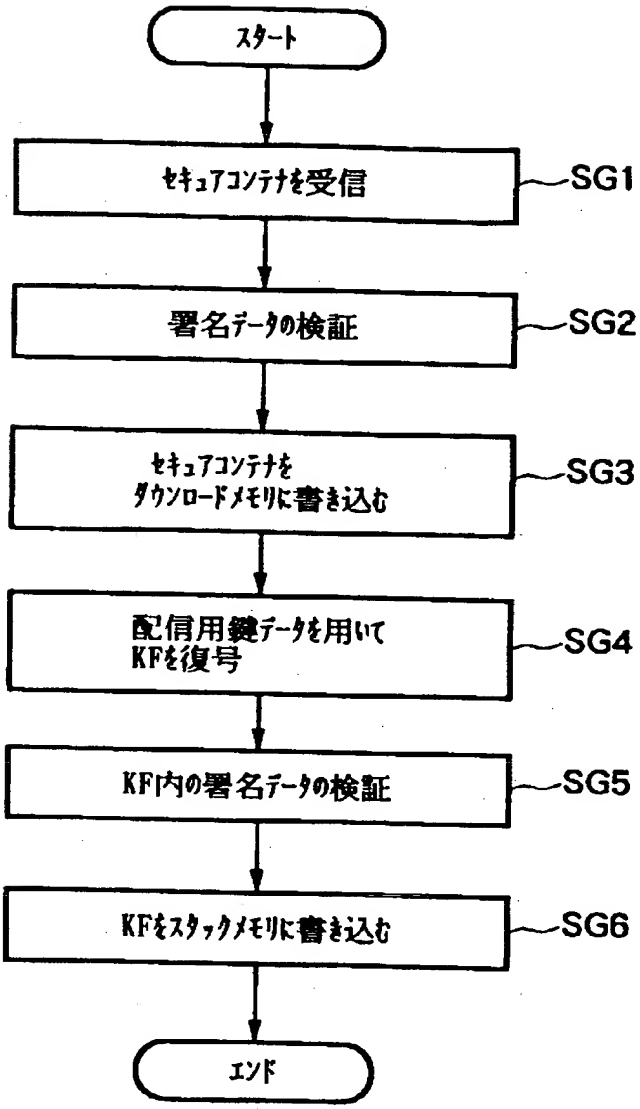

コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
105₁
165
購入・利用
形態操作部
S165
SAM
211
ダウンロード
メモリ(HDD)
(104)
810
ホストCPU
Kc,199,196,C
外部メモリ
201
163
復号・伸長モジュール
220
相互認証部
225
半開示処理部
199
221
224
伸長部
復号部(Kses)
C
C
電子透かし
情報処理部
Kc,C
222
223
復号部(Kc)
196
C
169
再生モジュール

【図２１】

記憶部192に記憶されるデータ



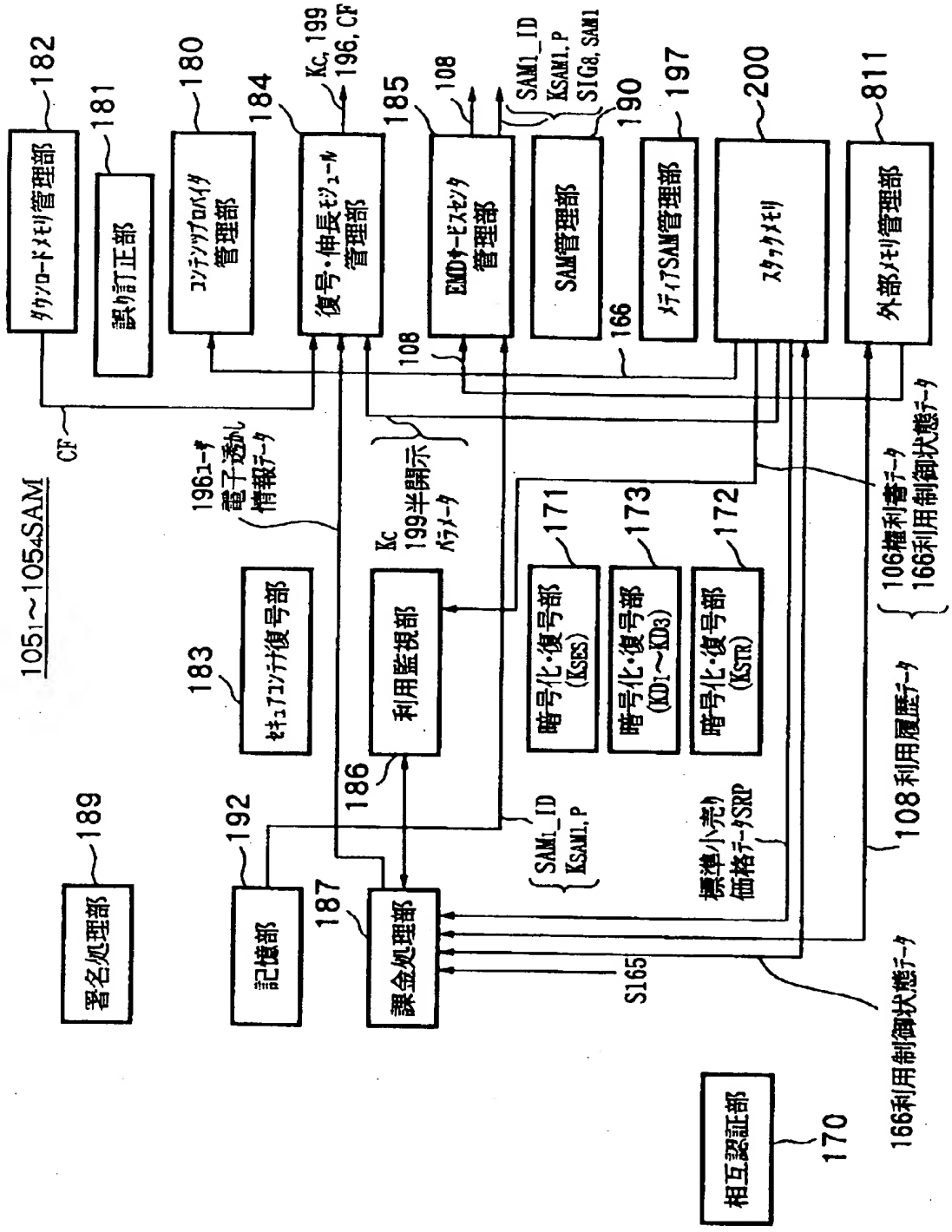
【図２２】



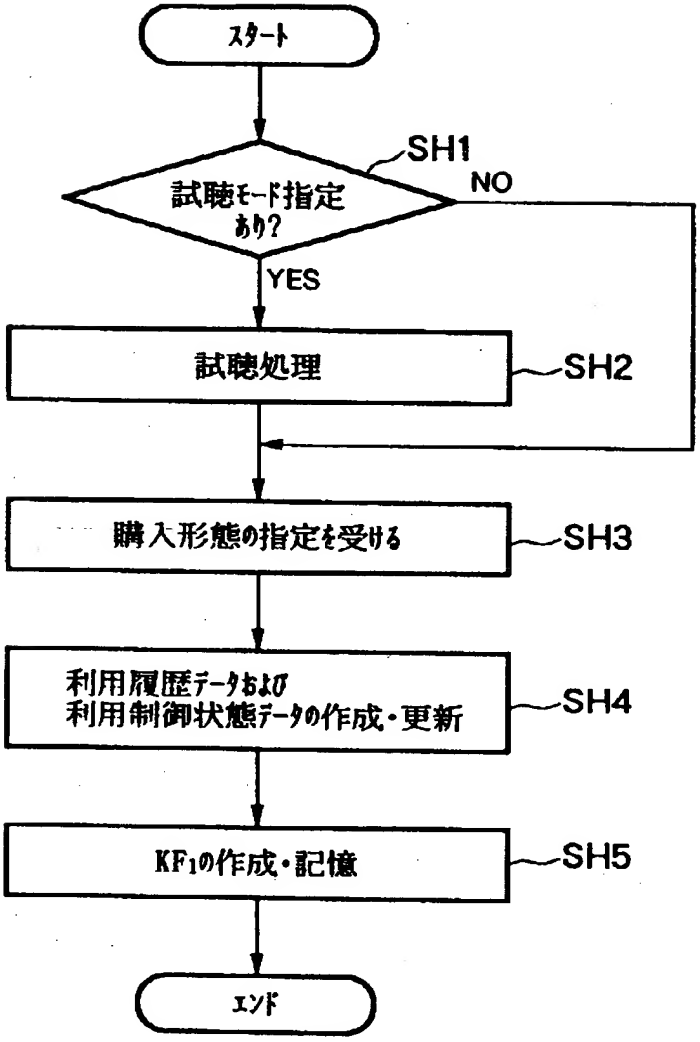
SAMにおけるKFの復号処理

出証特２０００－３０４３０２６

【図２３】

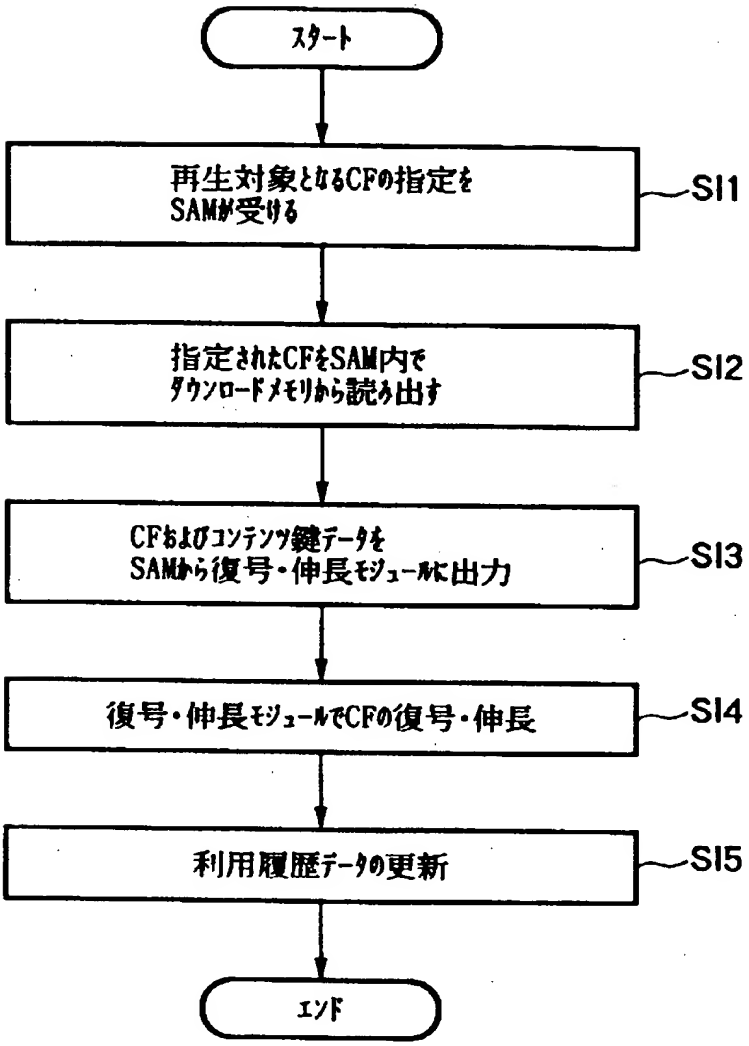

182
181
180
184
Kc, 199
196, CF
185
108
SAM1_ID
KSAM1, P
SIG8, SAM1
190
197
200
811
ダウンロードメモリ管理部
誤り訂正部
コンテンツプロバイダ管理部
復号・伸長モジュール管理部
EMDサービスセンタ管理部
SAM管理部
メディアSAM管理部
スタックメモリ
外部メモリ管理部
CF
105₁～105₄SAM
196₁ 電子透かし情報データ
Kc 199半開示パラメータ
106権利書データ
166利用制御状態データ
183
セキュアコンテナ復号部
利用監視部
暗号化・復号部 (KSES)
暗号化・復号部 (KD1～KD3)
暗号化・復号部 (KSTR)
171
173
172
186
SAM1_ID
KSAM1, P
標準小売り価格データSRP
108利用履歴データ
189
192
187
署名処理部
記憶部
課金処理部
S165
166利用制御状態データ
相互認証部
170

【図２４】



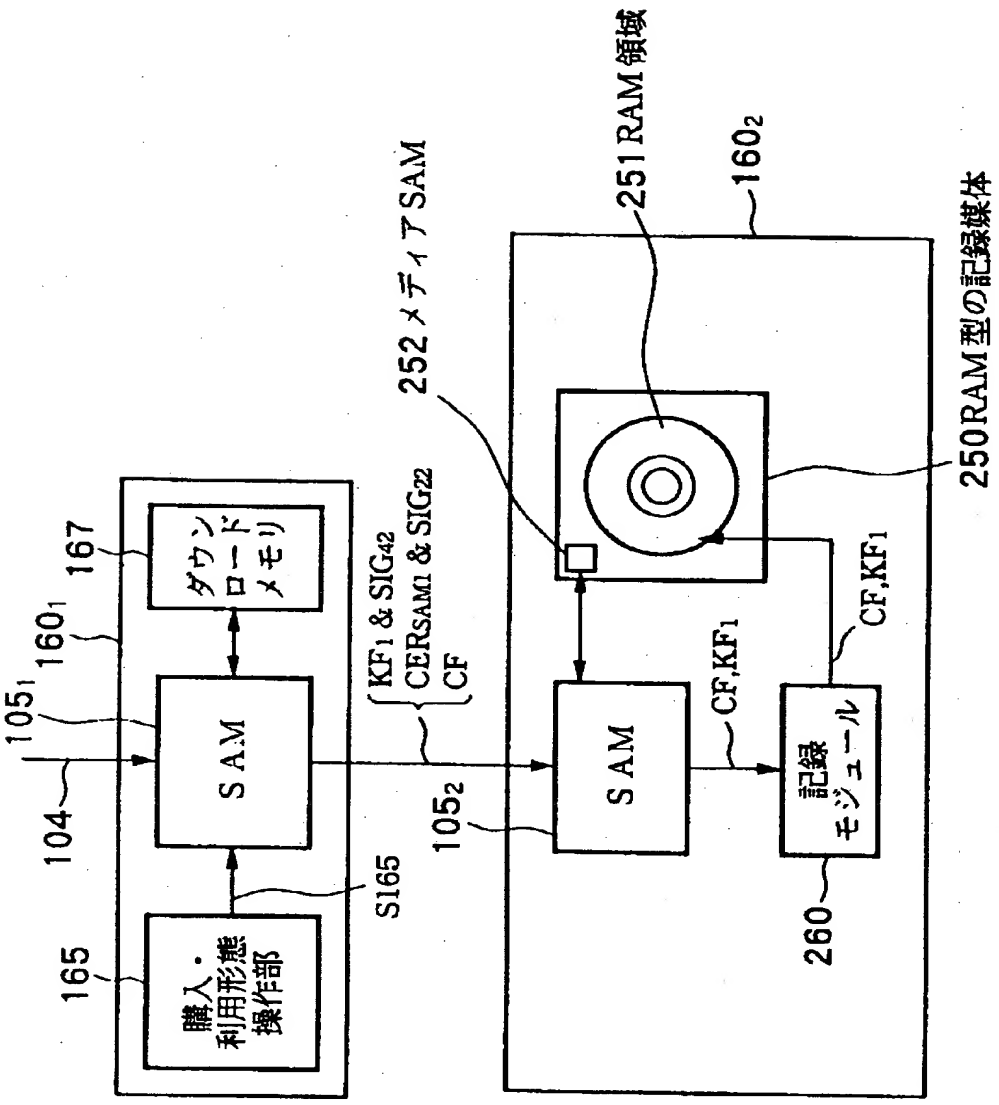
SAMにおけるセキュアコンテナの購入形態決定処理

【図２５】

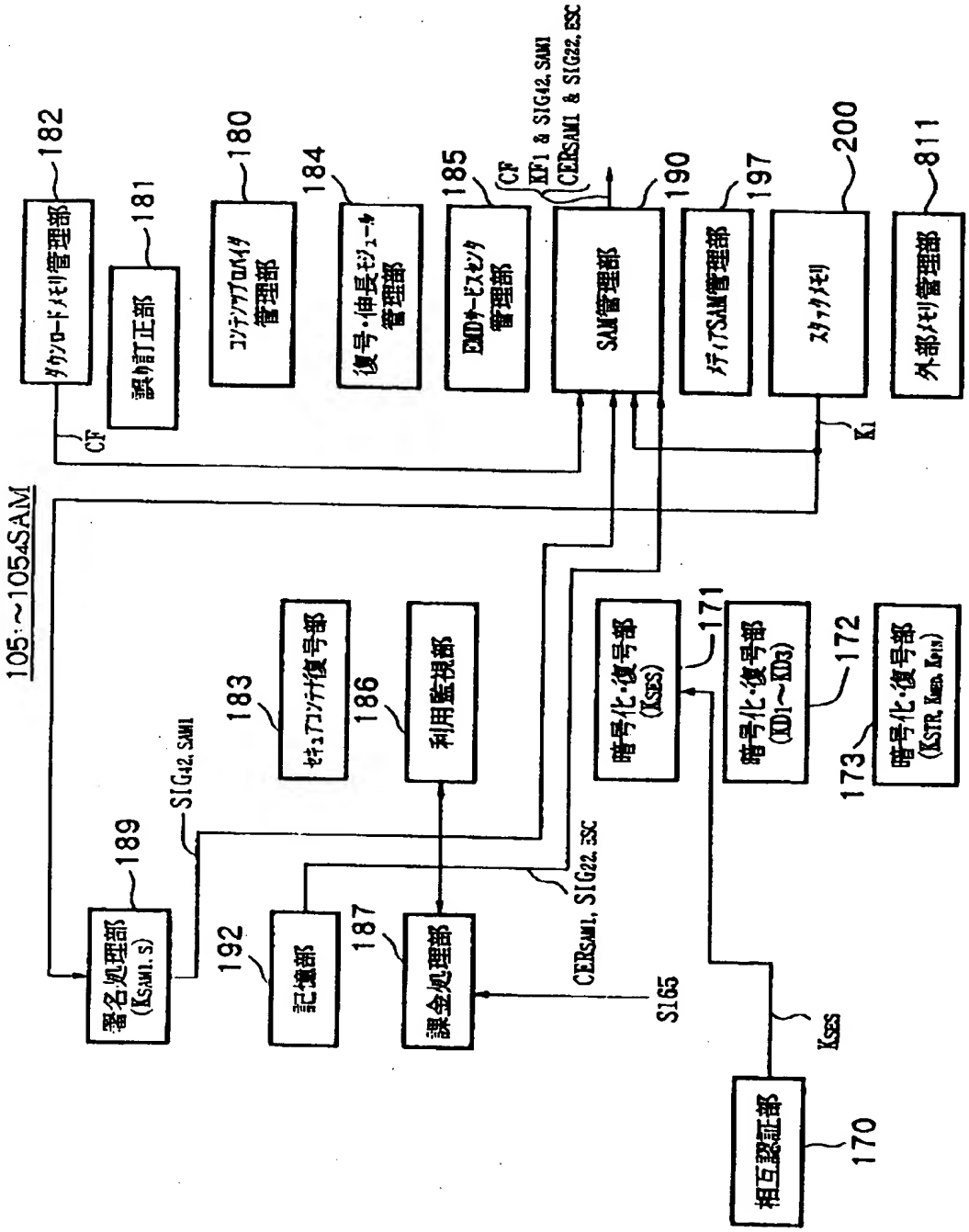


コンテンツデータの再生処理

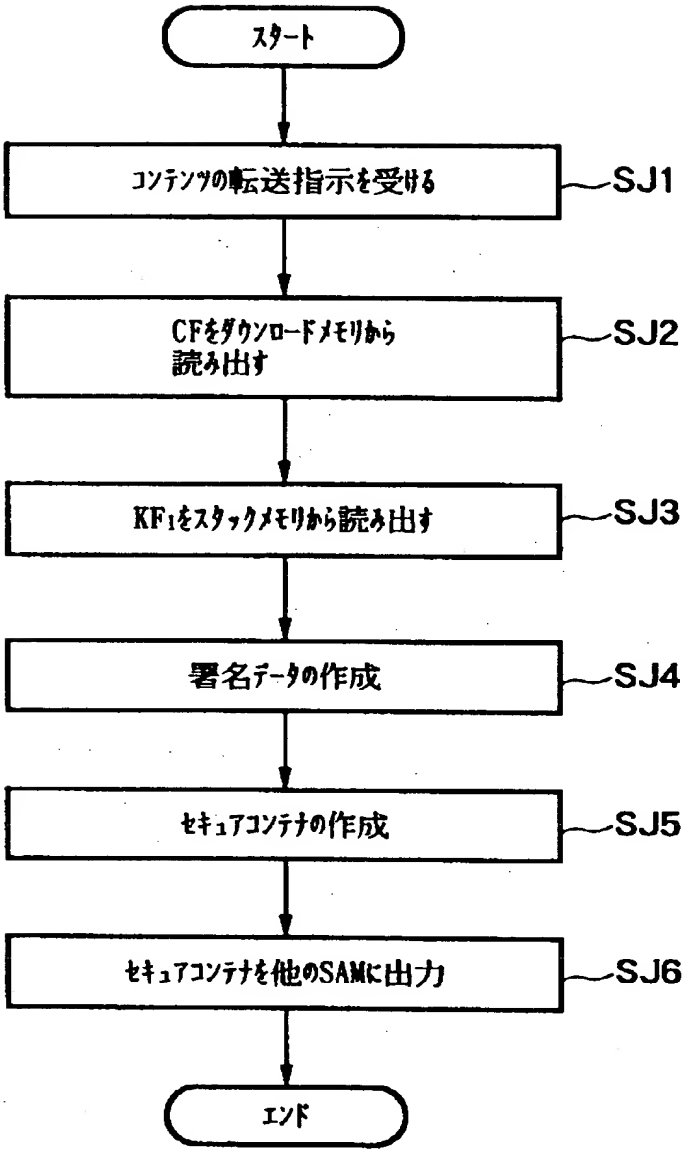
【図２６】


250RAM型の記録媒体
251 RAM領域
160_2
252 メディアSAM
KF_1 & SIG_{42}
CER_{SAM1} & SIG_{22}
CF
CF,KF_1
CF,KF_1
160_1
105_1
105_2
104
165
167
260
S165
SAM
SAM
記録モジュール
購入・利用形態操作部
ダウンロードメモリ

【図２７】

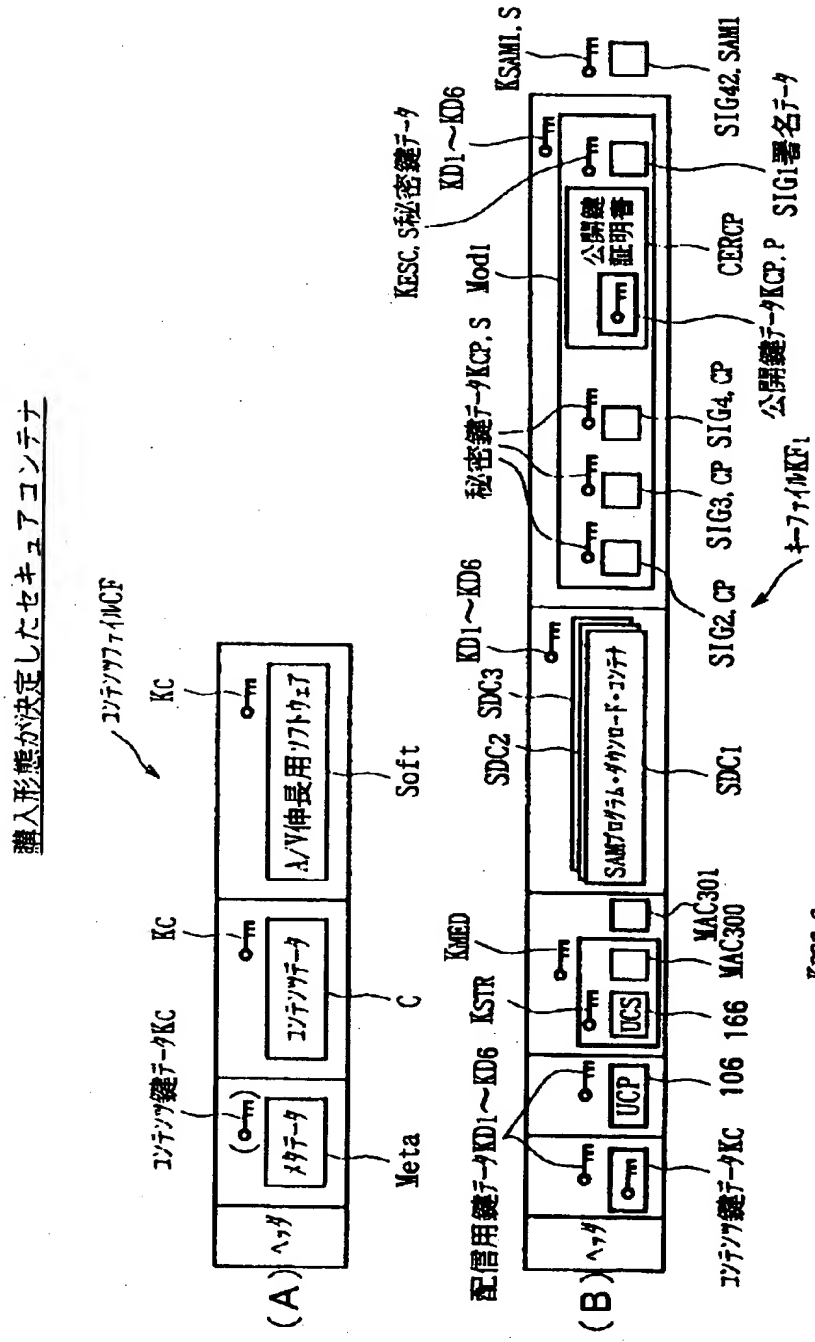

105:～105:SAM
182
ダウンロードメモリ管理部
181
誤り訂正部
180
コンテンツプロバイダ管理部
184
復号・伸長モジュール管理部
185
CF
KF1 & SIG42, SAM1
CERSAM1 & SIG22, ESC
EMDサービスセンタ管理部
190
SAM管理部
197
メディアSAM管理部
200
メインメモリ
811
外部メモリ管理部
CF
K1
183
セキュアコンテナ復号部
186
利用監視部
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMAC, KAES)
173
SIG42, SAM1
189
署名処理部 (KSAM1, S)
192
記憶部
187
課金処理部
CERSAM1, SIG22, ESC
S165
KSES
相互認証部
170

【図２８】

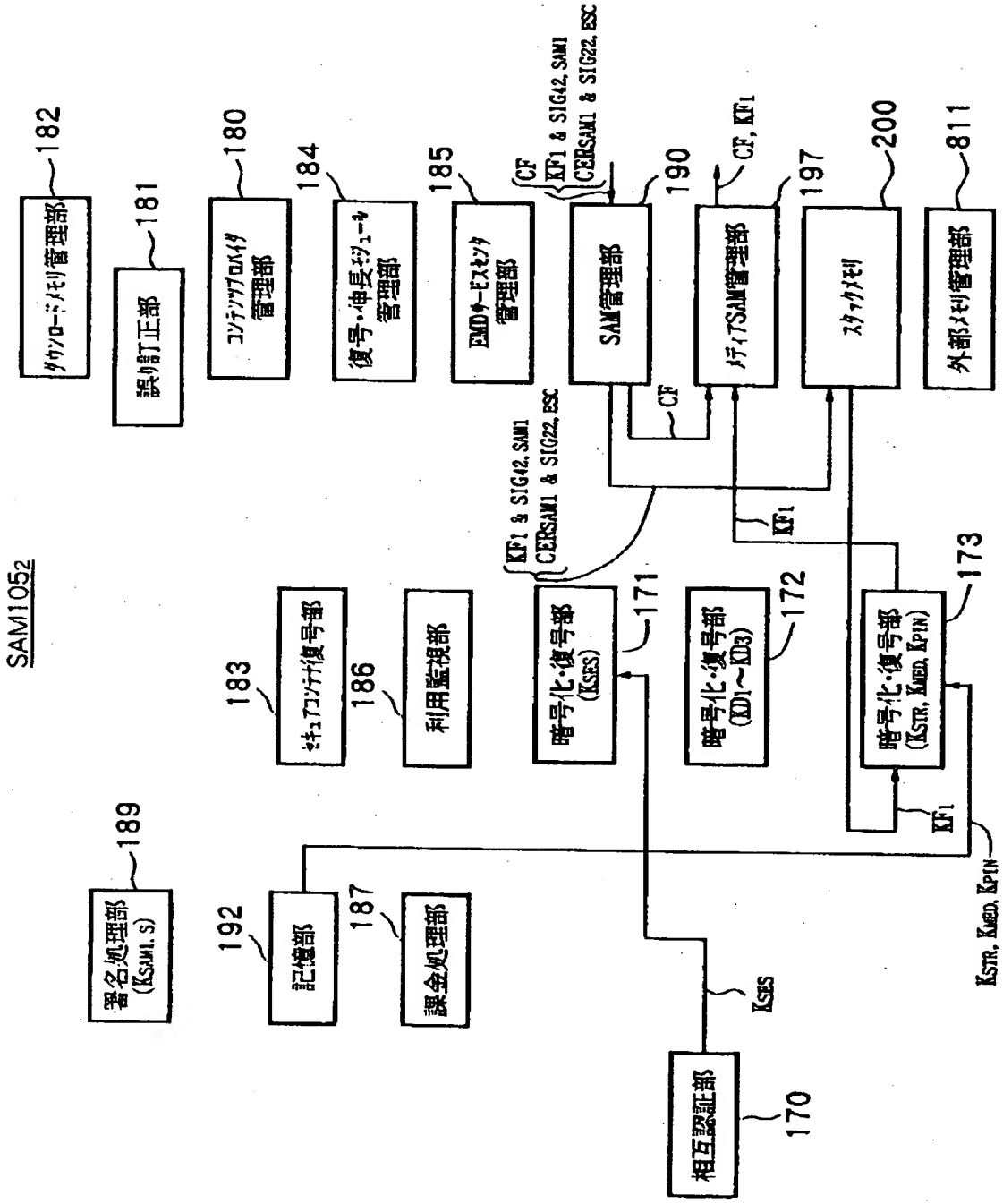


購入形態決定後のコンテンツを他のSAMに転送するSAMの処理

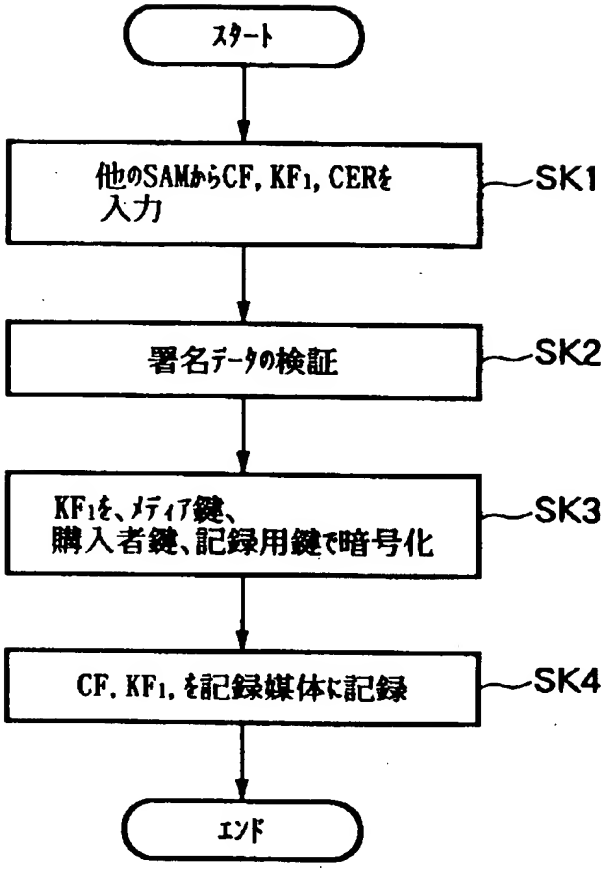
【図２９】


購入形態が決定したセキュアコンテナ
コンテンツファイルMCF
KC
コンテンツ鍵データKc
コンテンツデータ
A/V伸長用ソフトウェア
ヘッダ
メタデータ
Meta
C
Soft
(A)
KESC, S秘密鍵データ
KD1～KD6
KSAM1, S
Mod1
秘密鍵データKCP, S
公開鍵証明書
SIG42, SAM1
CERCP
SIG4, CP
SIG3, CP
公開鍵データKCP, P
SIG1署名データ
キーファイルKF1
SIG2, CP
KD1～KD6
SDC3
SDC2
SAMプログラム・ダウンロード・コンテナ
SDC1
KMED
KSTR
UCS
UCP
MAC301
MAC300
106
166
配信用鍵データKD1～KD6
コンテンツ鍵データKc
ヘッダ
(B)
KESC, S
SIG22, ESC
公開鍵証明書
KSAM1, P
CERSAM1
(C)

【図３０】

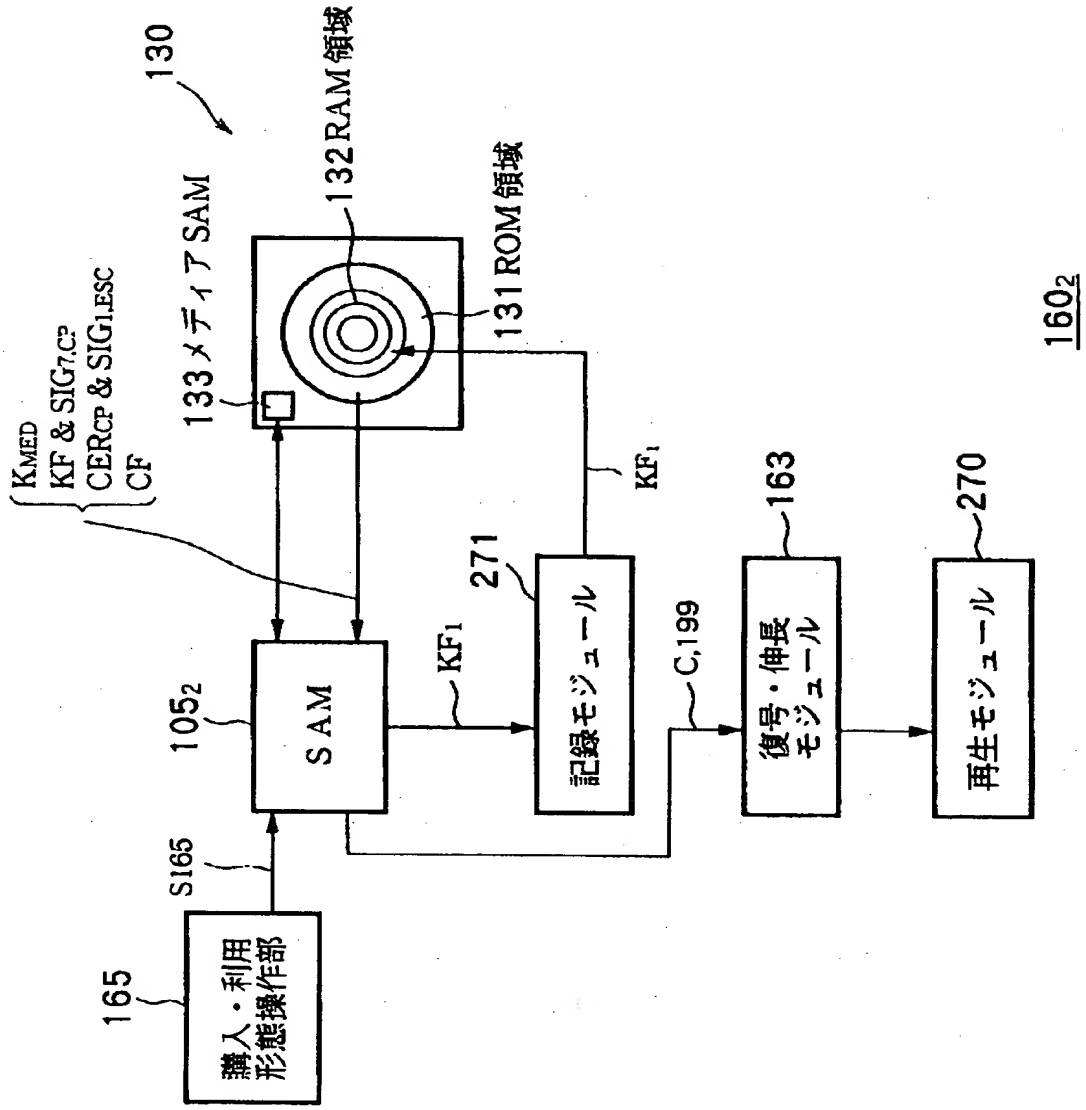

SAM105₂
182
ダウンロードメモリ管理部
181
誤り訂正部
180
コンテンツプロバイダ管理部
184
復号・伸長エンジン管理部
185
EMDサービスセンタ管理部
CF
KF1 & SIG42, SAM1
CERSAM1 & SIG22, ESC
190
SAM管理部
CF, KF1
197
ポイントSAM管理部
200
スタックメモリ
811
外部メモリ管理部
KF1 & SIG42, SAM1
CERSAM1 & SIG22, ESC
CF
KF1
183
ポイント計算部
186
利用監視部
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KPIN)
173
KF1
189
署名処理部 (KSAM1, S)
192
記憶部
187
課金処理部
KSES
KSTR, KMED, KPIN
相互認証部
170

【図３１】

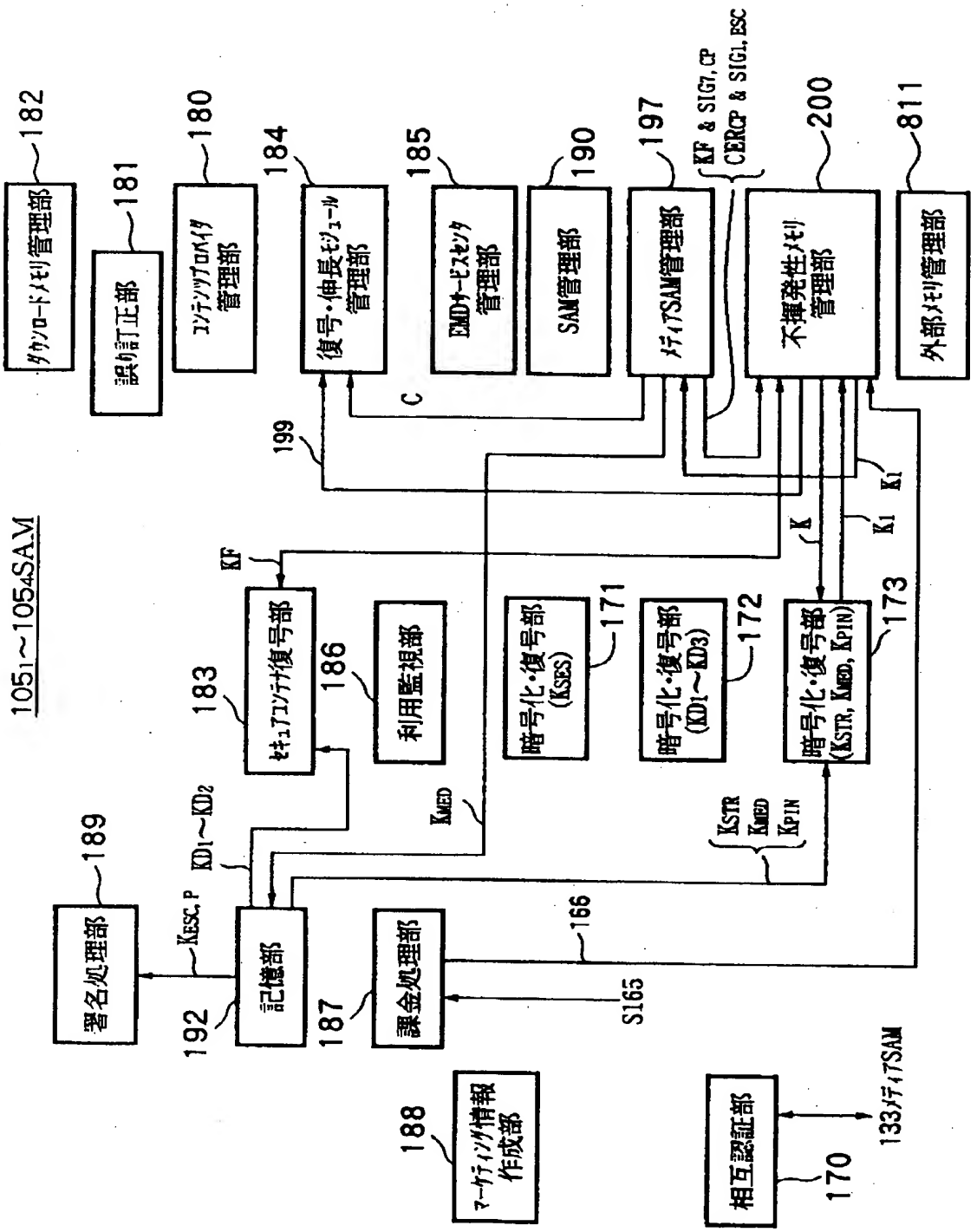


他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

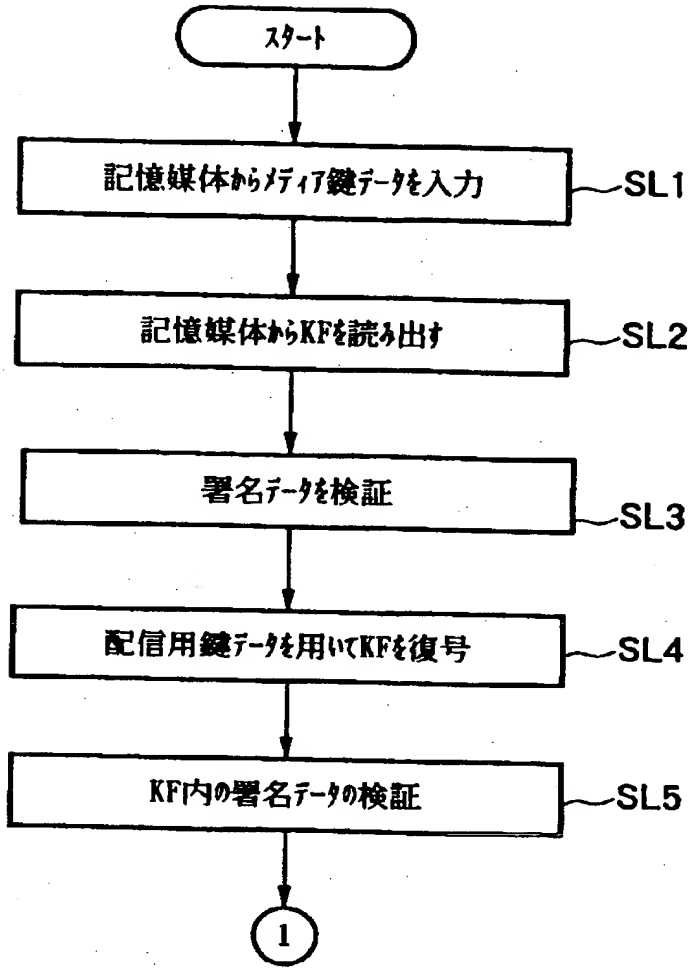
【図３２】


130
132 RAM領域
131 ROM領域
133 メディア SAM
K_{MED}
KF & $SIG_{7,CP}$
CER_{CP} & $SIG_{1,ESC}$
CF
KF_1
271
記録モジュール
163
復号・伸長モジュール
270
再生モジュール
160_2
105_2
SAM
KF_1
C,199
S165
165
入・利用形態操作部

【図３３】

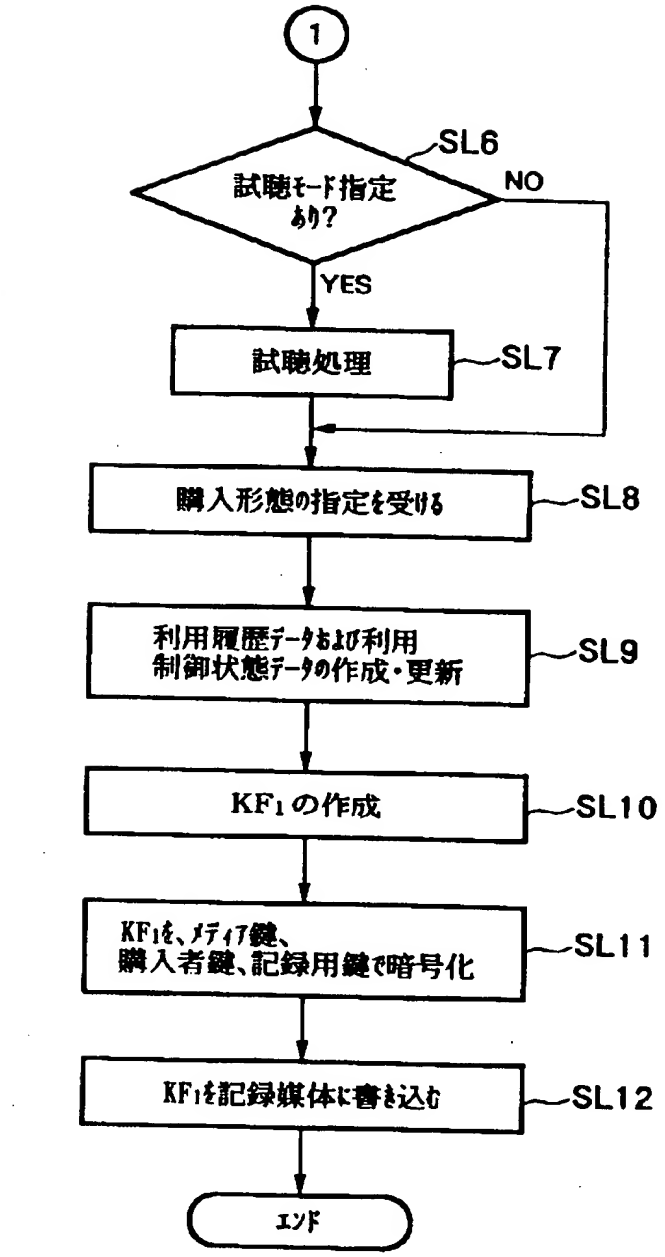

ダウンロードメモリ管理部
182
誤り訂正部
181
コンテンツプロバイダ管理部
180
復号・伸長モジュール管理部
184
EMDサービスセンタ管理部
185
SAM管理部
190
メディアSAM管理部
197
不揮発性メモリ管理部
200
外部メモリ管理部
811
KF & SIG7, CP
CERCP & SIG1, ESC
C
199
K
K1
K1
KF
105₁～105₄SAM
セキュアコンテナ復号部
183
利用監視部
186
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KPIN)
173
KD1～KD2
KMED
KSTR
KMED
KPIN
署名処理部
189
KESC, P
記憶部
192
課金処理部
187
166
S165
マーケティング情報作成部
188
相互認証部
170
133メディアSAM

【図３４】



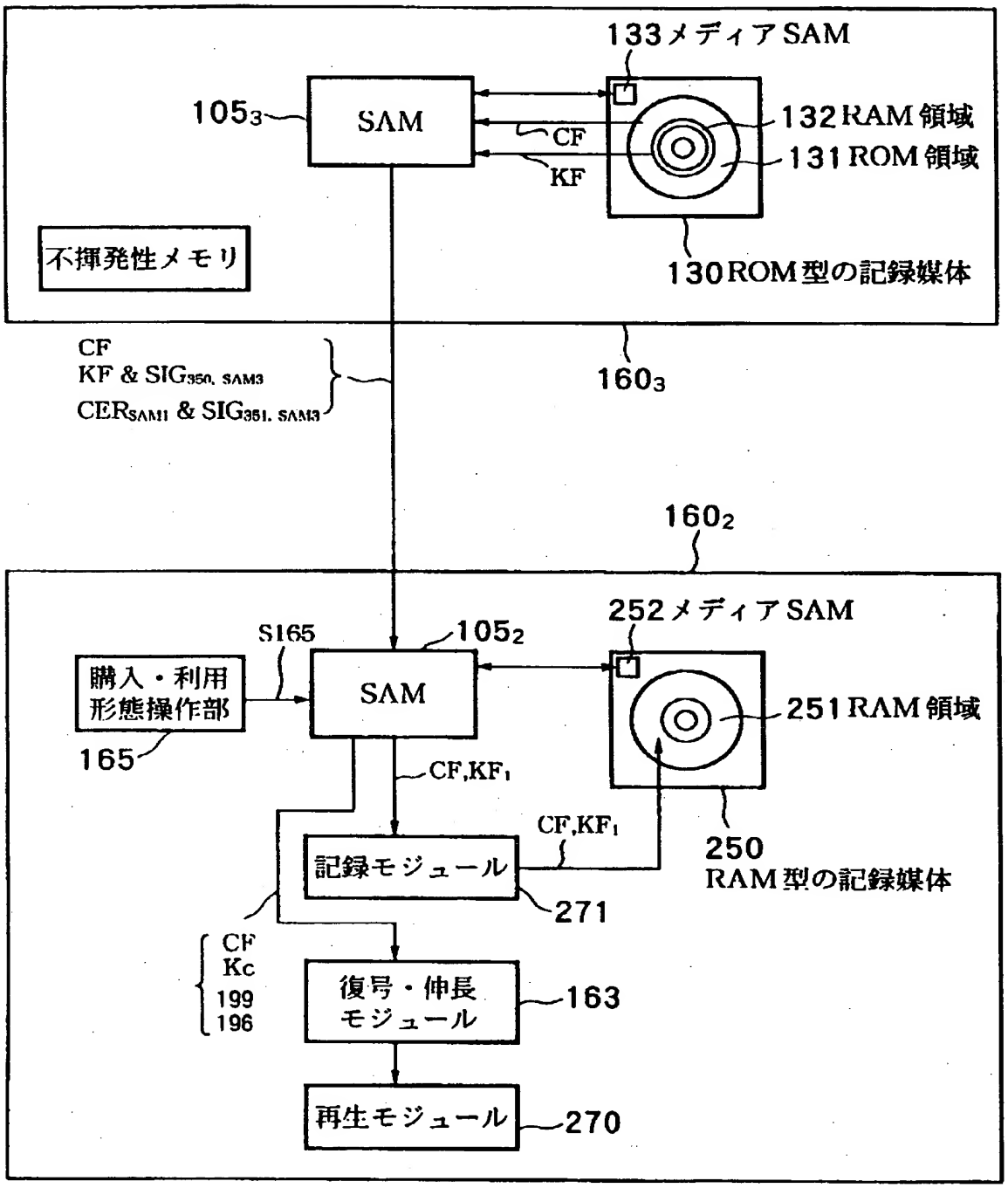
オンラインで配給されたコンテンツのSAMにおける購入形態決定処理

【図３５】

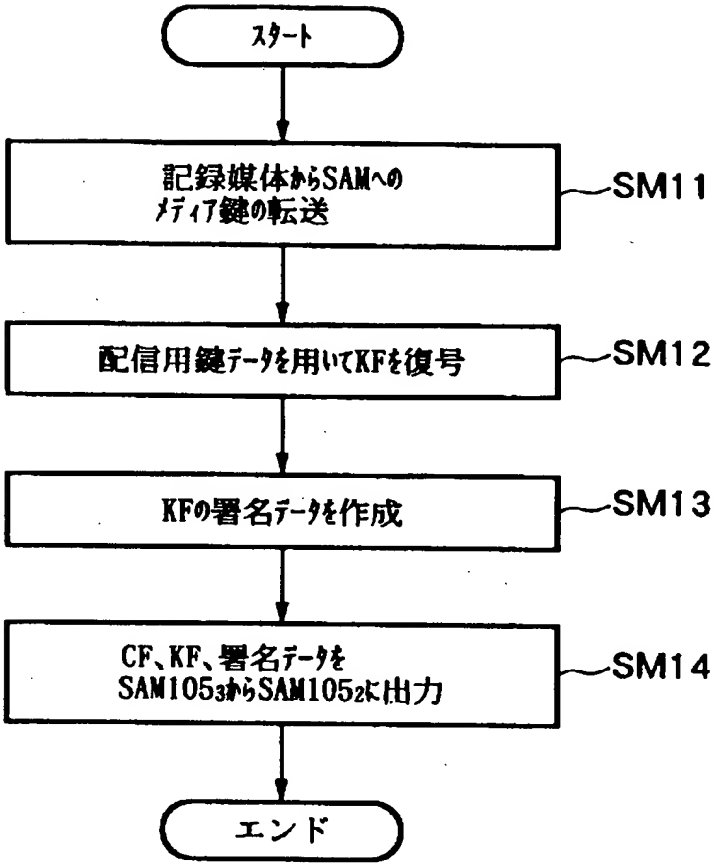


オフラインで配給されたコンテンツのSAMにおける購入形態決定処理

【図３６】

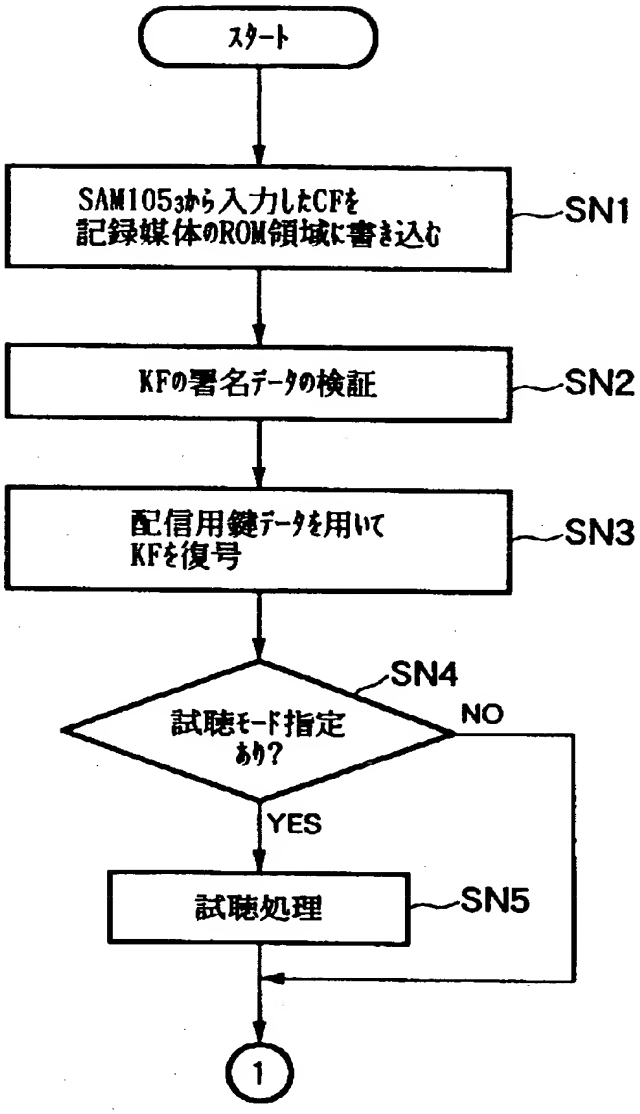

133メディアSAM
105_3
SAM
CF
KF
132RAM領域
131ROM領域
不揮発性メモリ
130ROM型の記録媒体
CF
KF & $SIG_{350,\ SAM3}$
CER_{SAM1} & $SIG_{351,\ SAM3}$
160_3
160_2
252メディアSAM
S165
105_2
購入・利用
形態操作部
SAM
251RAM領域
165
CF,KF_1
CF,KF_1
250
RAM型の記録媒体
記録モジュール
271
CF
Kc
199
196
復号・伸長
モジュール
163
再生モジュール
270

【図３７】



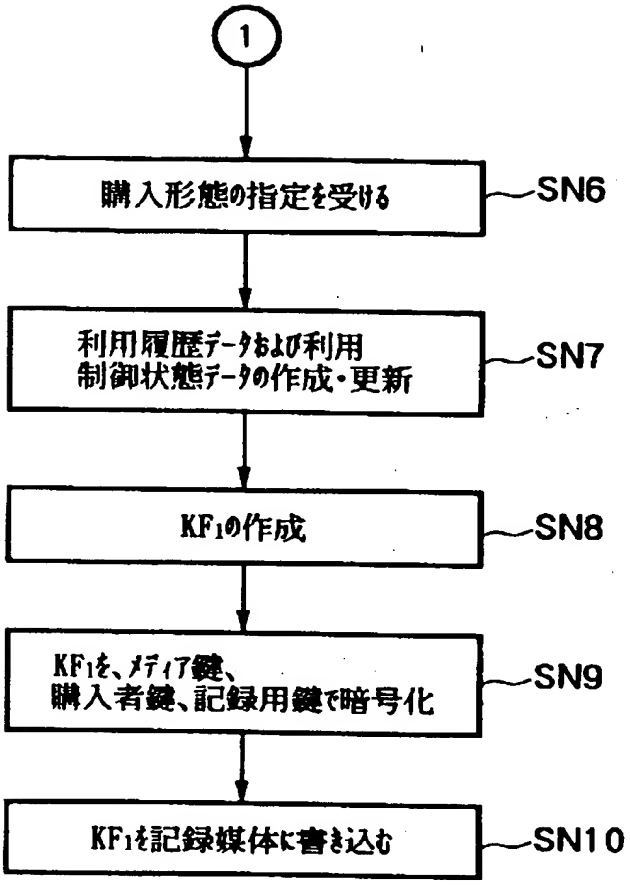
SAM105$_3$の処理

【図３８】



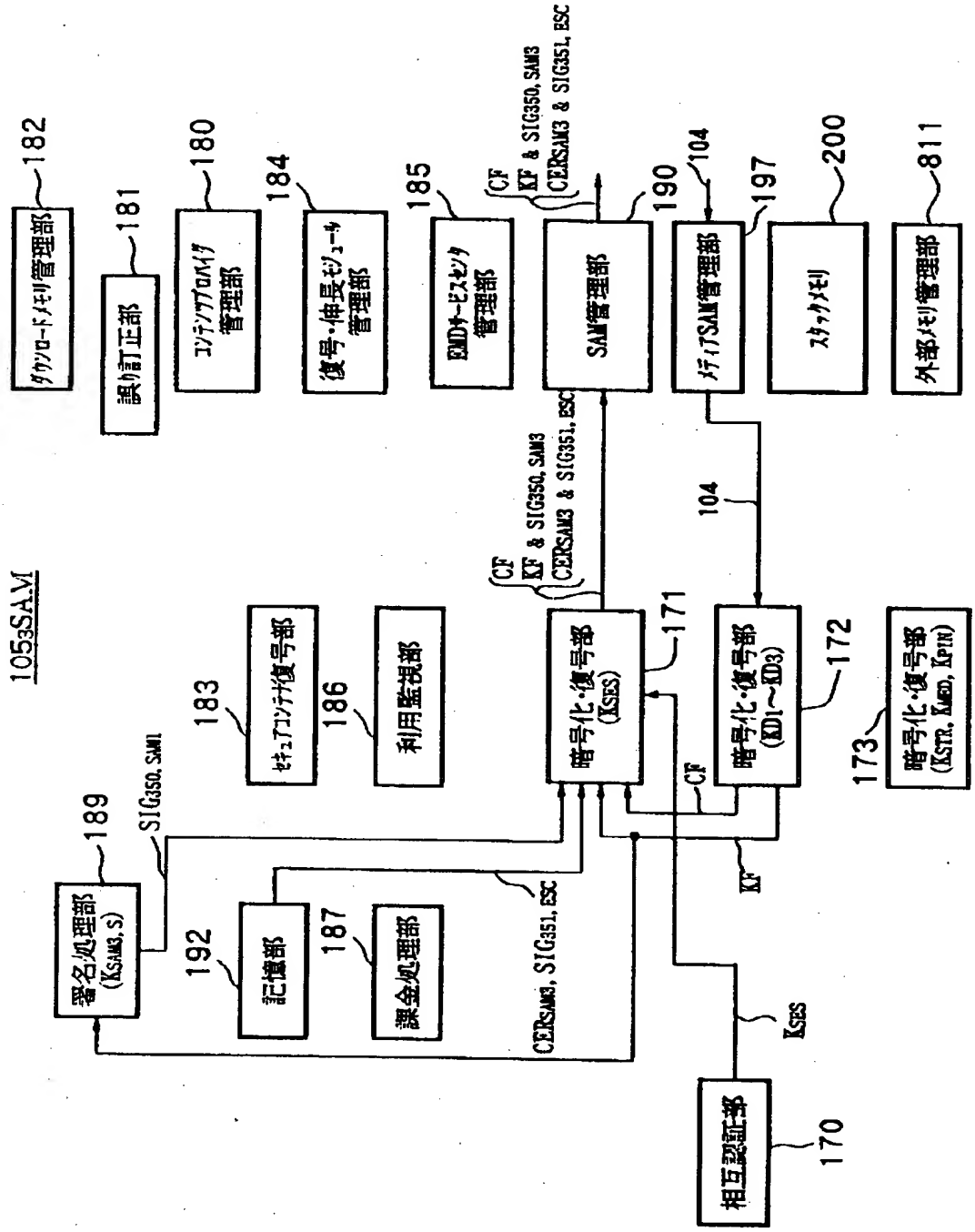
SAM105₂の処理

【図３９】

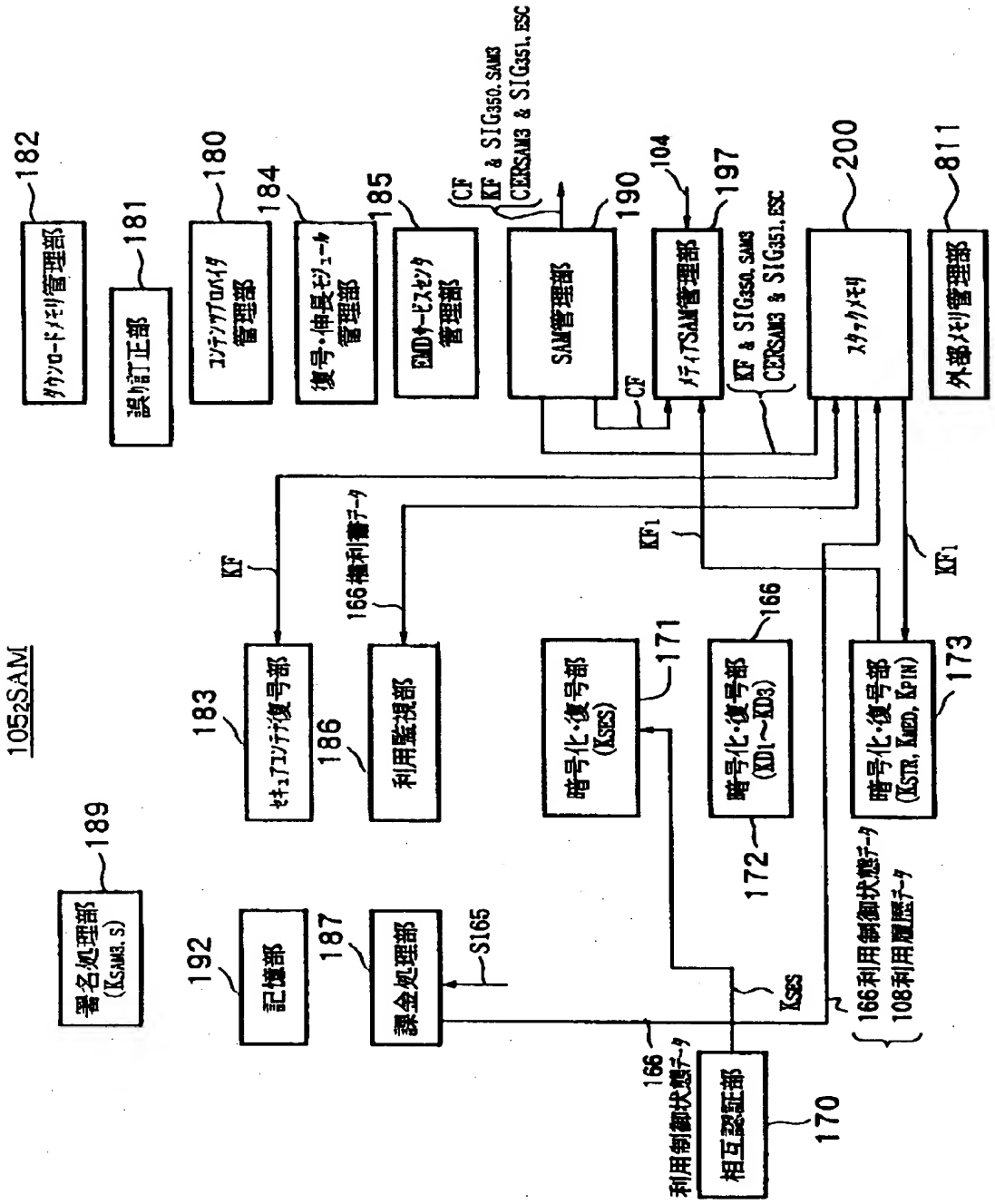


SAM105₂の処理

【図４０】

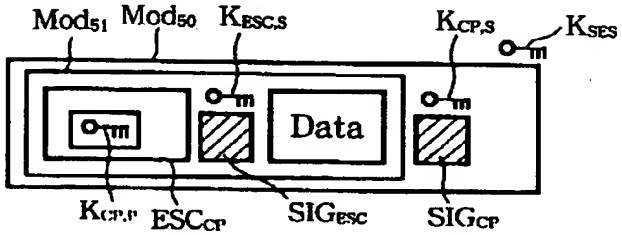

105₃SAM
182
ダウンロードメモリ管理部
181
誤り訂正部
180
コンテンツプロバイダ管理部
184
復号・伸長モジュール管理部
185
EMDサービスセンタ管理部
CF
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
190
SAM管理部
104
197
メディアSAM管理部
200
スタックメモリ
811
外部メモリ管理部
CF
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
104
183
セキュアコンテナ復号部
186
利用監視部
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
172
173
暗号化・復号部 (KSTR, KMED, KPIN)
CF
KF
189
署名処理部 (KSAM3, S)
SIG350, SAM1
192
記憶部
187
課金処理部
CERSAM3, SIG351, ESC
KSES
相互認証部
170

【図４１】

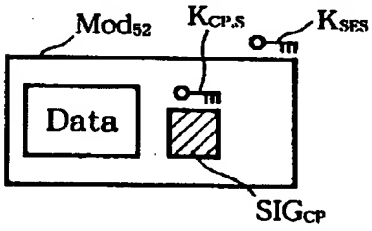

105₂SAM
182
ダウンロードメモリ管理部
181
誤り訂正部
180
コンテンツプロバイダ管理部
184
復号・伸長モジュール管理部
185
EMDサービスセンタ管理部
CF
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
190
SAM管理部
104
197
バディSAM管理部
200
スタックメモリ
811
外部メモリ管理部
KF
166権利書データ
KF1
183
セキュアコンテナ復号部
186
利用監視部
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
166
暗号化・復号部 (KSTR, KMED, KPIN)
173
189
署名処理部 (KSAM3, S)
192
記憶部
187
課金処理部
S165
172
KSES
166利用制御状態データ
108利用履歴データ
166利用制御状態データ
相互認証部
170

【図４２】

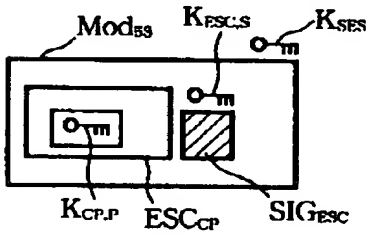
（A） 101(CP)→SAM105$_1$
(イン・バンド)



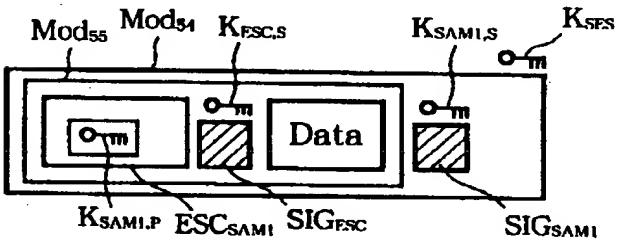
（B） 101(CP)→SAM105$_1$
(アウト・オブ・バンド)



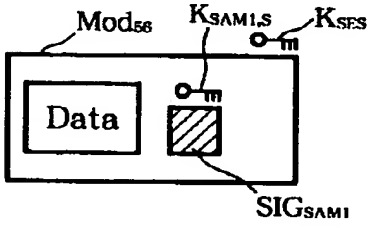
（C） 102(ESC)→SAM105$_1$
(アウト・オブ・バンド)



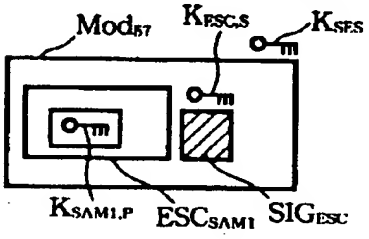
（D） SAM105$_1$→101(CP)
(イン・バンド)



（E） SAM105$_1$→101(CP)
(アウト・オブ・バンド)

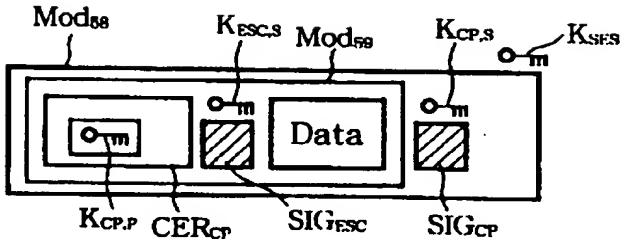


（F） 102(ESC)→101(CP)
(アウト・オブ・バンド)

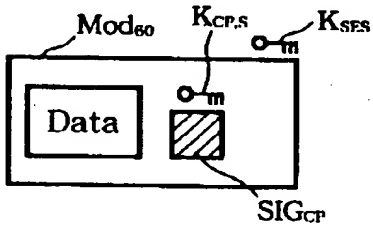


【図４３】

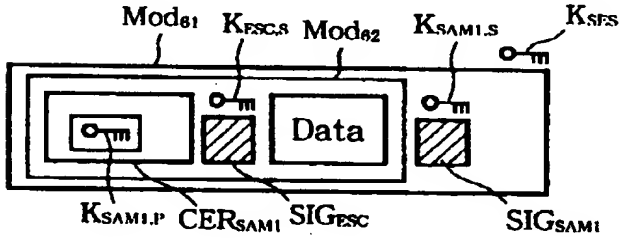
（G） 101(CP)→102(ESC)
(イン・バンド)



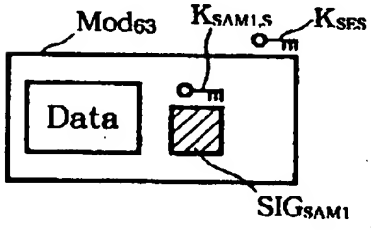
（H） 101(CP)→102(ESC)
(アウト・オブ・バンド)



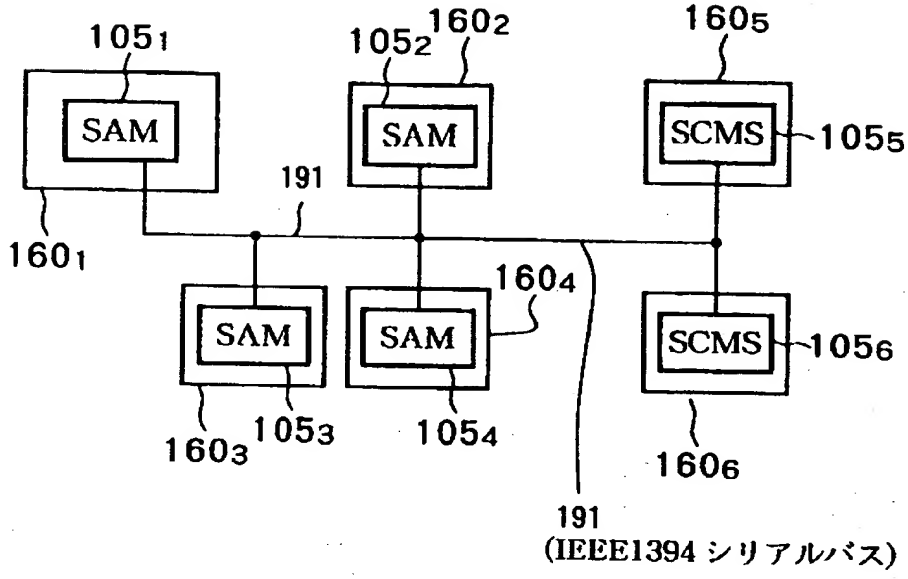
（I） SAM105$_1$→102(ESC)
(イン・バンド)



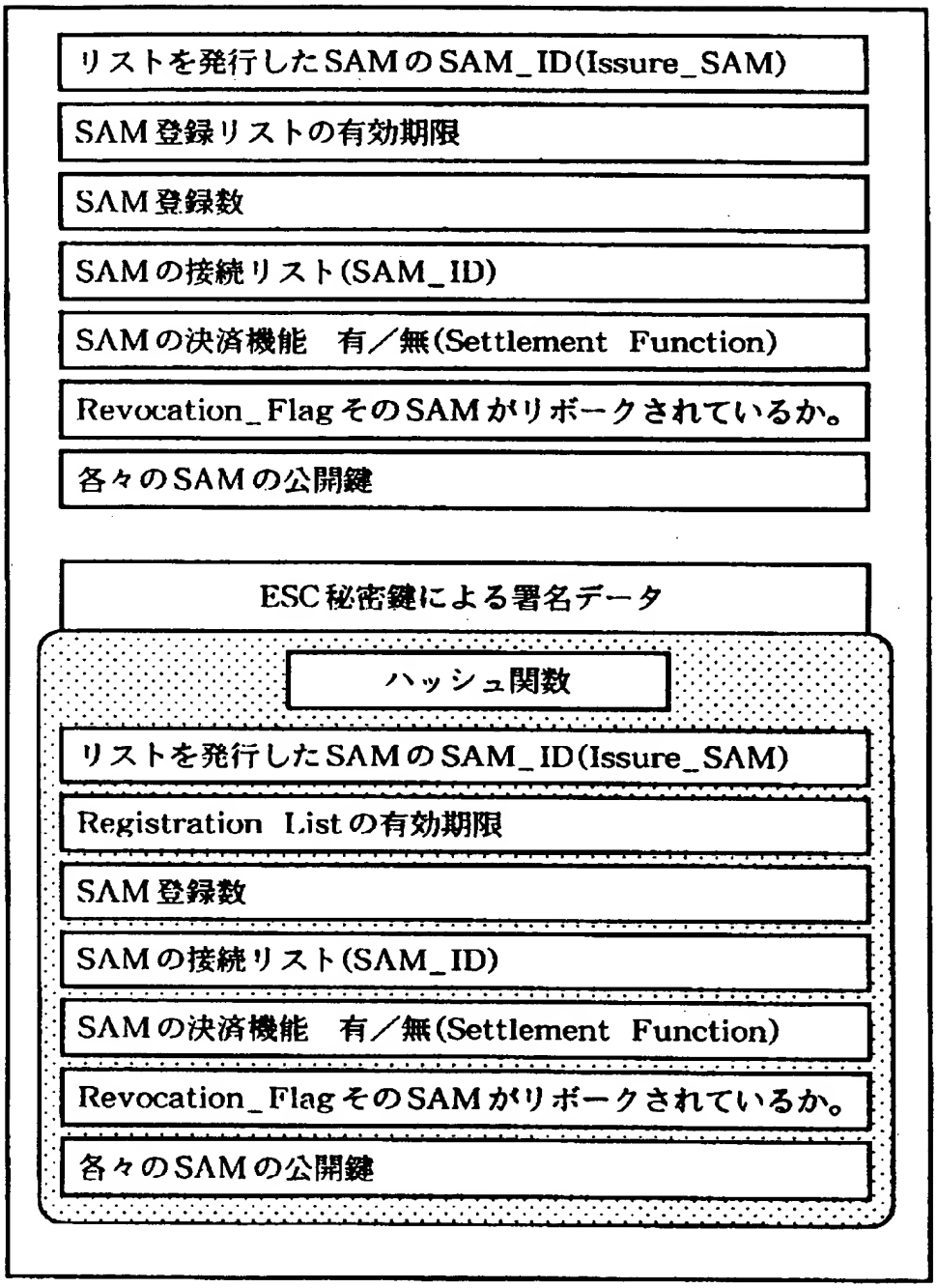
（J） SAM105$_1$→102(ESC)
(アウト・オブ・バンド)



【図４４】

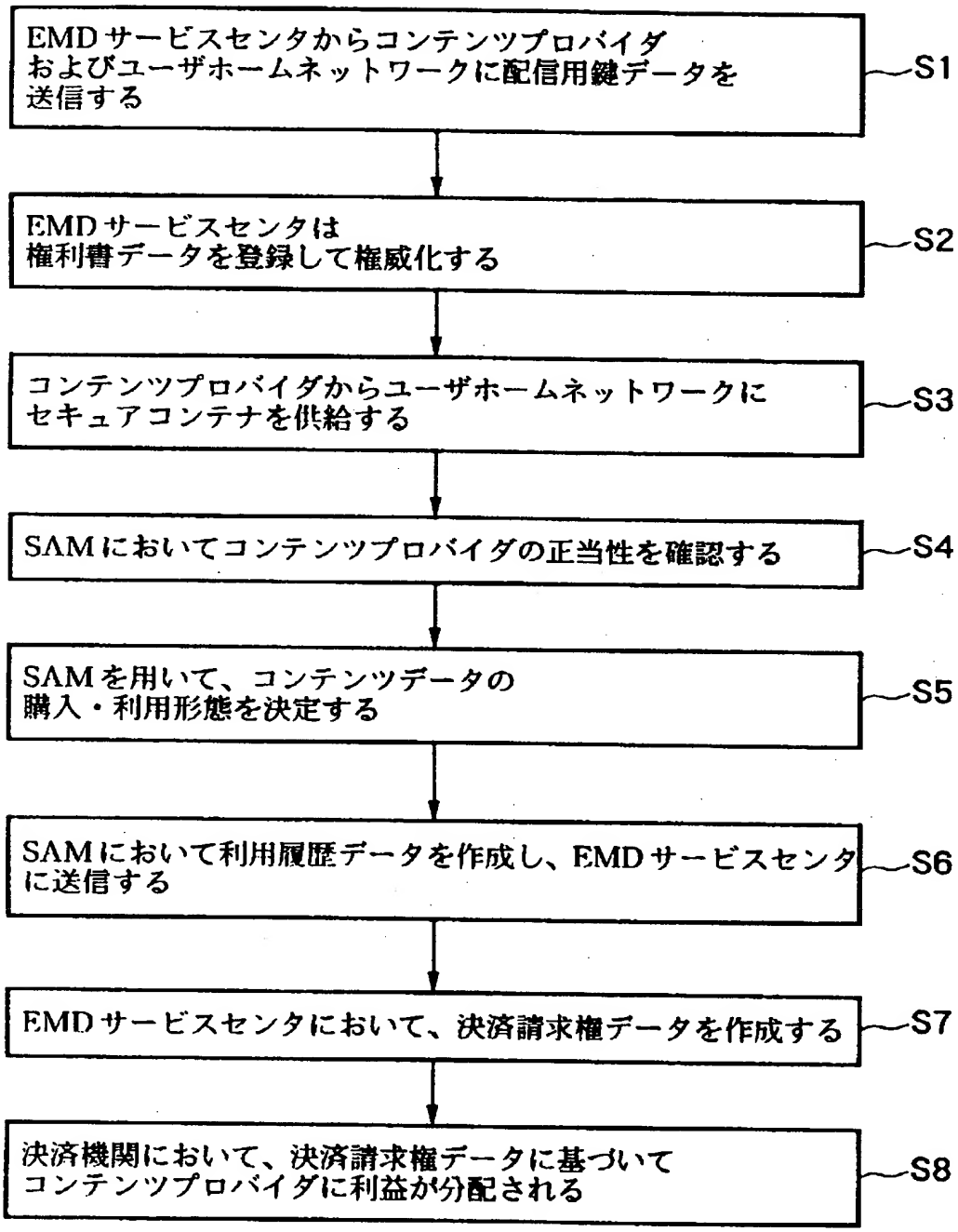

105_1
105_2
160_2
160_5
SAM
SAM
SCMS
105_5
191
160_1
160_4
SAM
SAM
SCMS
105_6
160_3
105_3
105_4
160_6
191
(IEEE1394 シリアルバス)

【図４５】

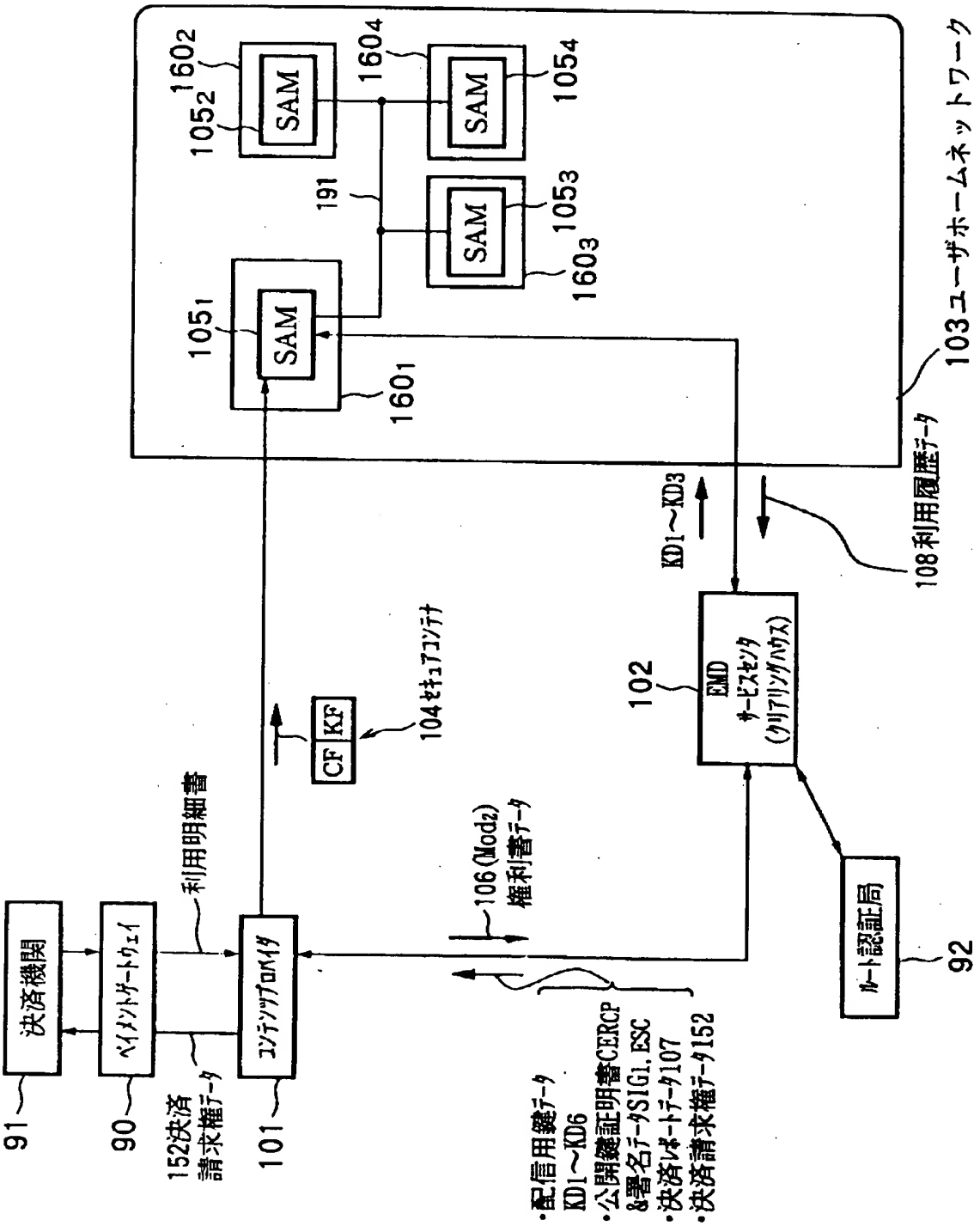


SAM登録リスト

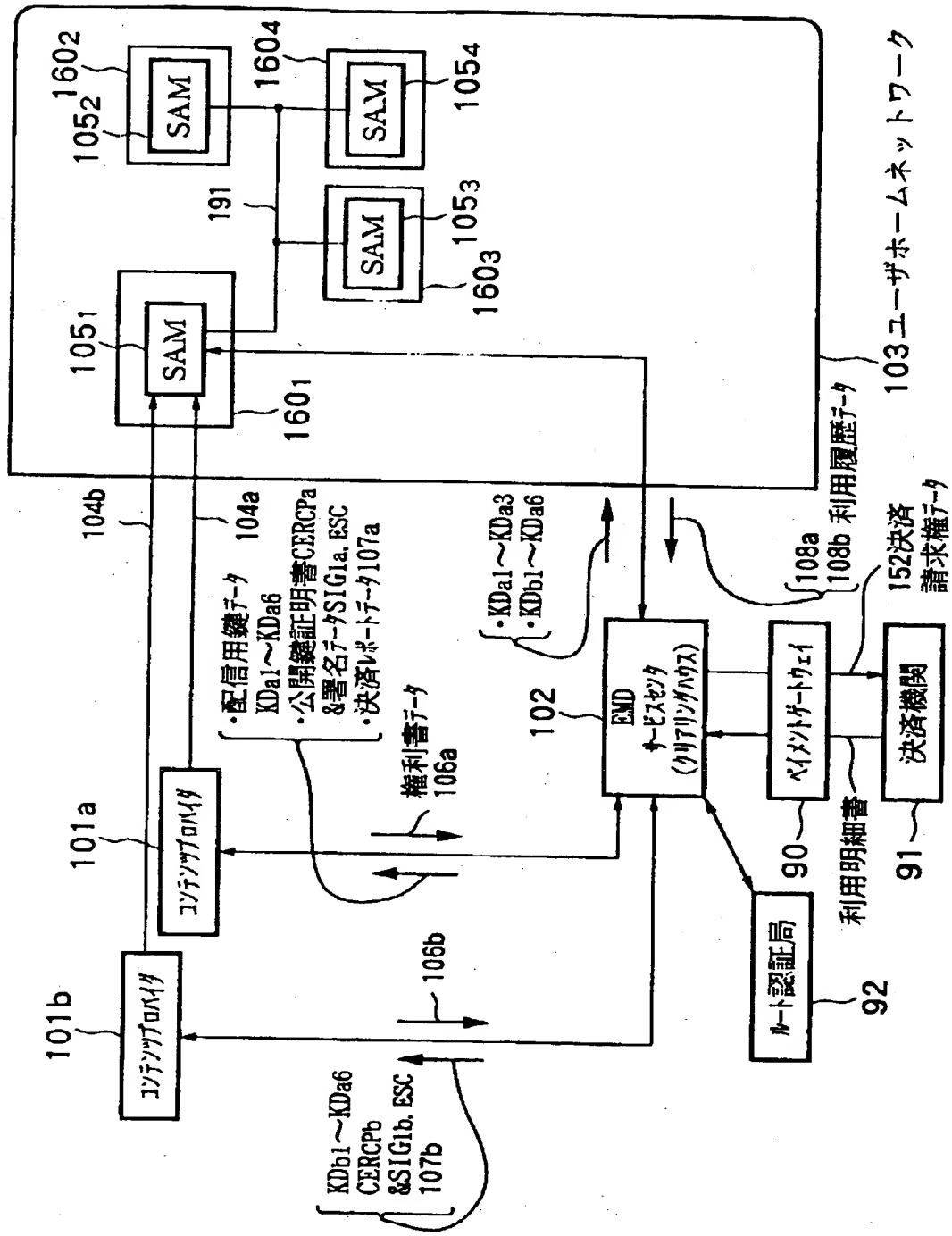
【図４６】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークに配信用鍵データを送信する
S1
EMDサービスセンタは権利書データを登録して権威化する
S2
コンテンツプロバイダからユーザホームネットワークにセキュアコンテナを供給する
S3
SAMにおいてコンテンツプロバイダの正当性を確認する
S4
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S5
SAMにおいて利用履歴データを作成し、EMDサービスセンタに送信する
S6
EMDサービスセンタにおいて、決済請求権データを作成する
S7
決済機関において、決済請求権データに基づいてコンテンツプロバイダに利益が分配される
S8

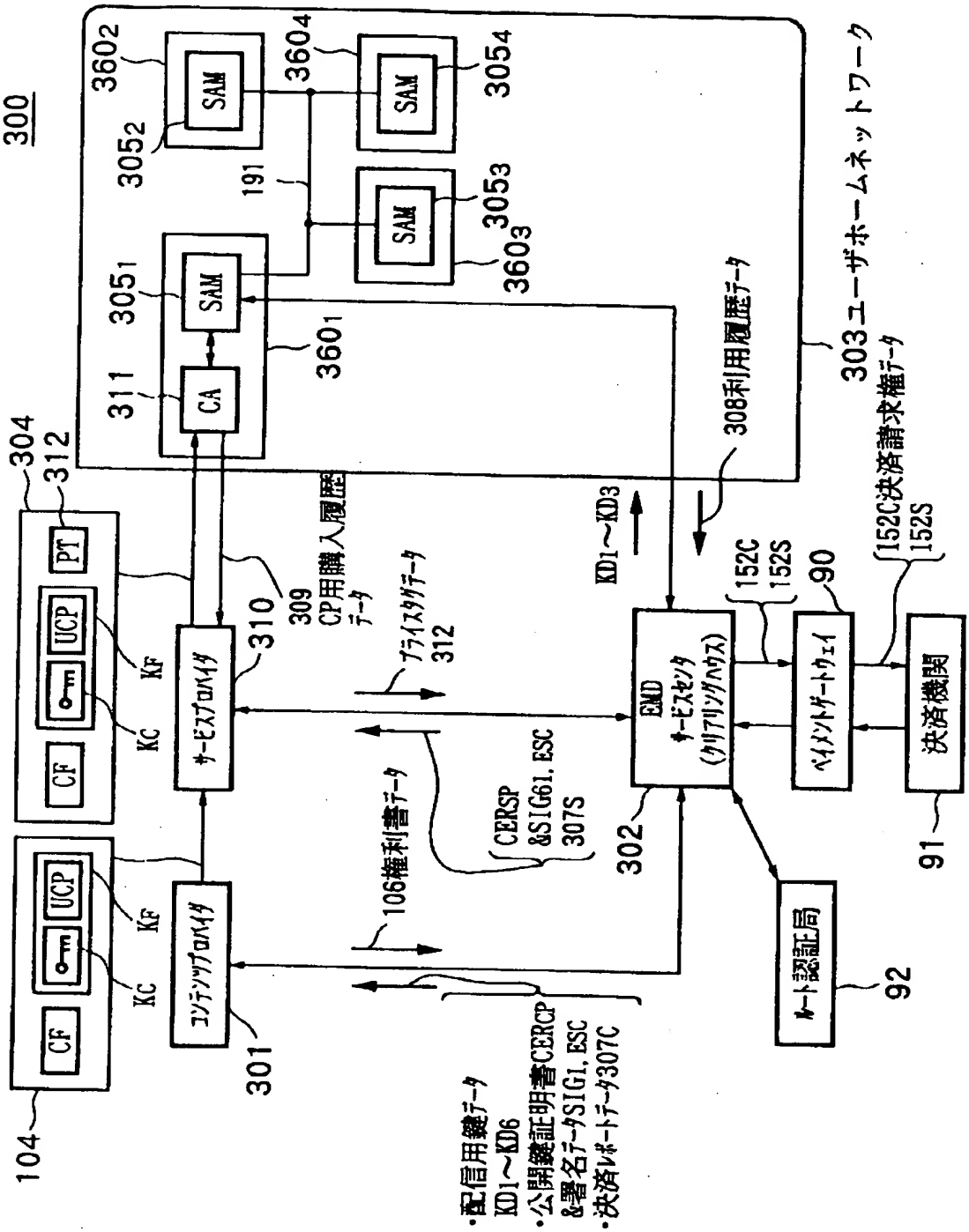
【図４７】


決済機関
ペイメントゲートウェイ
コンテンツプロバイダ
91
90
101
152決済
請求権データ
利用明細書
CF
KF
104セキュアコンテナ
106(Mod2)
権利書データ
EMD
サービスセンタ
(クリアリングハウス)
102
KD1～KD3
108利用履歴データ
103ユーザホームネットワーク
SAM
1052
1602
1604
1054
191
1053
1603
1051
1601
ルート認証局
92
・配信用鍵データ
KD1～KD6
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107
・決済請求権データ152

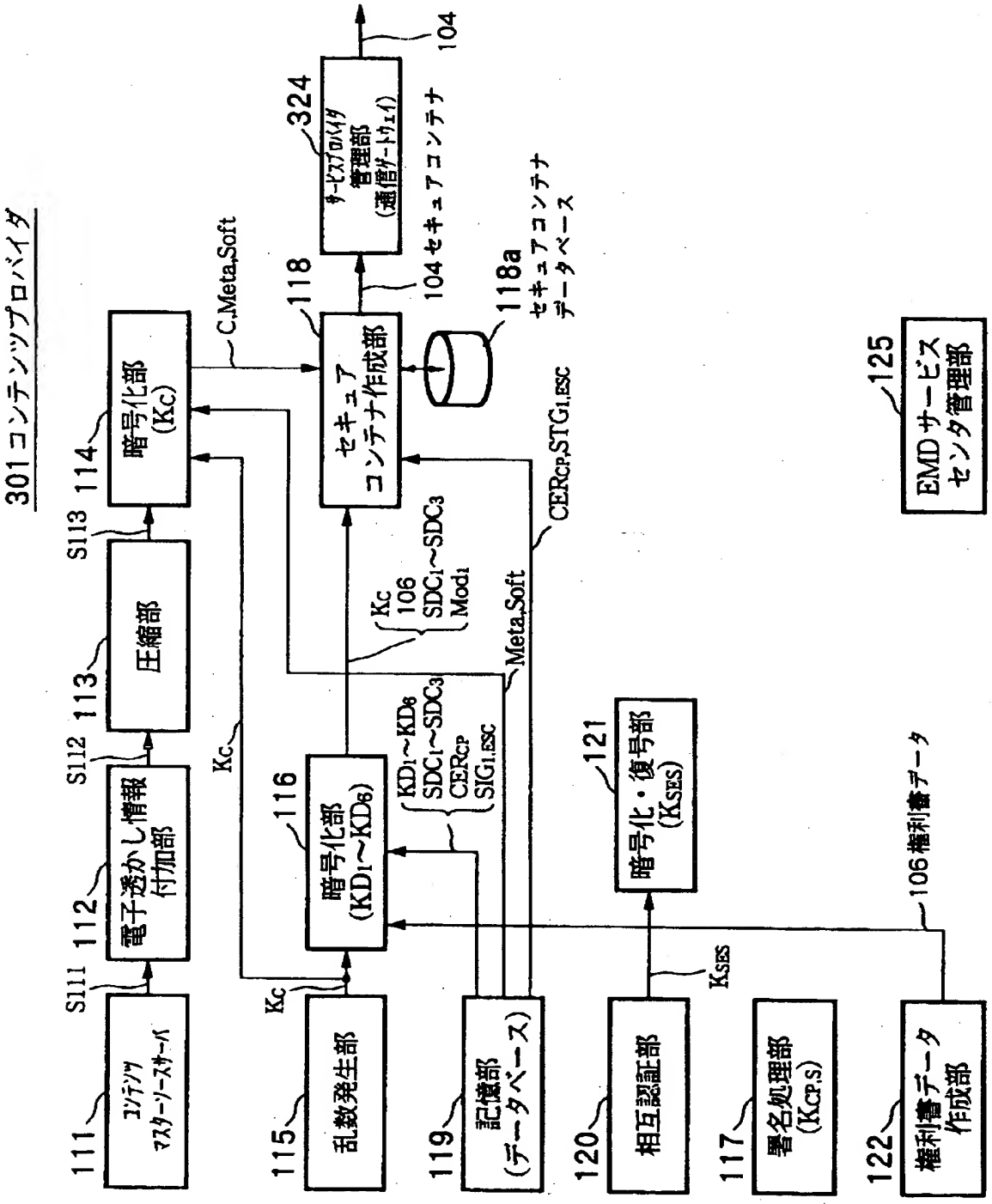
【図４８】


SAM
SAM
SAM
SAM
191
EMD
サービスセンタ
(クリアリングハウス)
ペイメントゲートウェイ
決済機関
ルート認証局
エンテンツプロバイダ
エンテンツプロバイダ
103ユーザホームネットワーク
・配信用鍵データ
KDa1～KDa6
・公開鍵証明書CERCPa
&署名データSIG1a, ESC
・決済レポートデータ107a
権利書データ
106a
106b
KDb1～KDa6
CERCPb
&SIG1b, ESC
107b
・KDa1～KDa3
・KDb1～KDa6
108a
108b 利用履歴データ
152決済
請求権データ
利用明細書
90
91
92
101a
101b
102
104a
104b

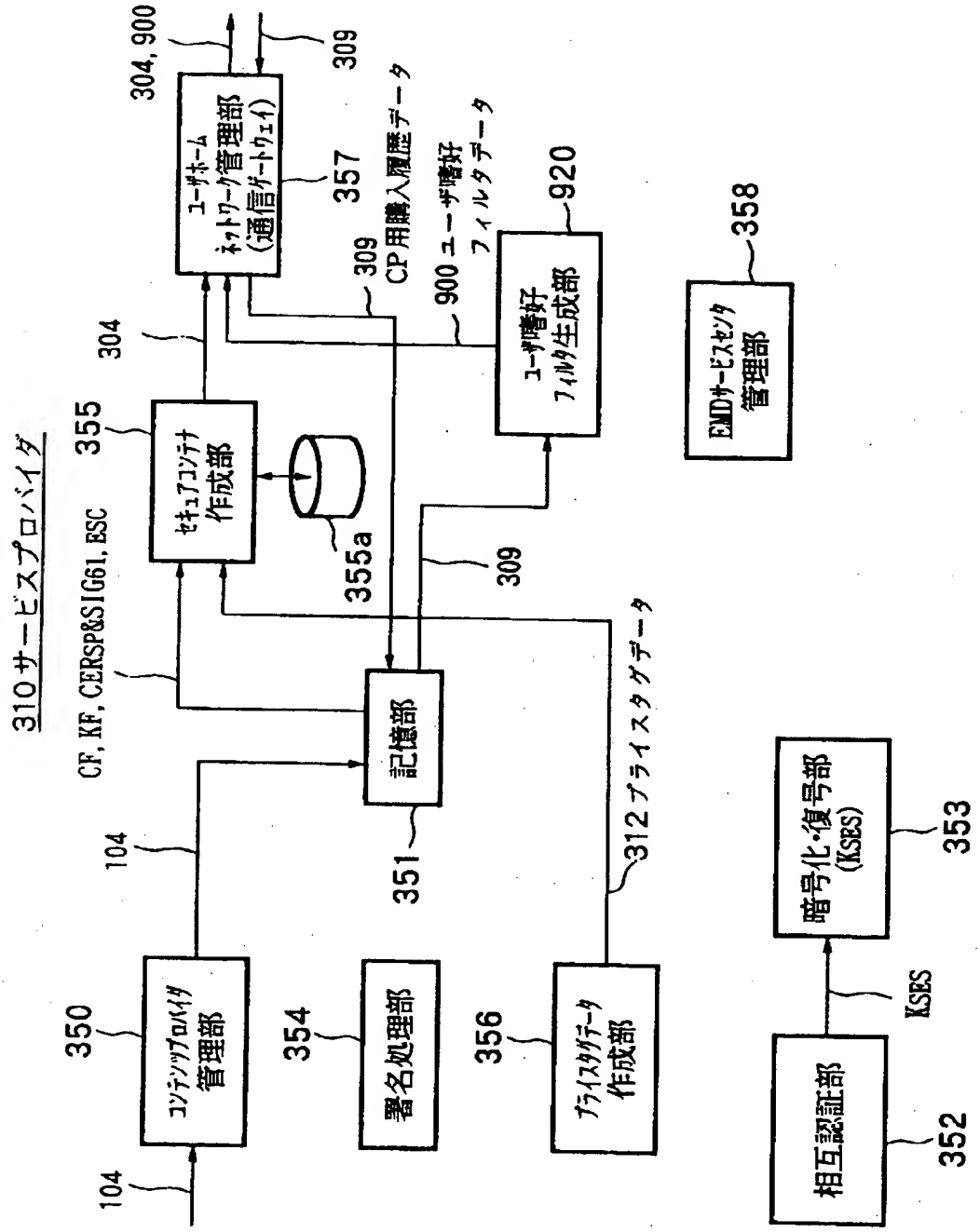
【図４９】


300
SAM
CA
PT
UCP
CF
KF
KC
サービスプロバイダ
コンテンツプロバイダ
EMD
サービスセンタ
(クリアリングハウス)
ペイメントゲートウェイ
決済機関
ルート認証局
ユーザホームネットワーク
CP用購入履歴データ
プライスタグデータ
利用履歴データ
KD1～KD3
106権利書データ
CERSP
&SIG61, ESC
307S
152C
152S
152C決済請求権データ
・配信用鍵データ
KD1～KD6
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ307C
104
301
302
303
304
309
310
311
312
90
91
92
191
3601
3602
3603
3604
3051
3052
3053
3054

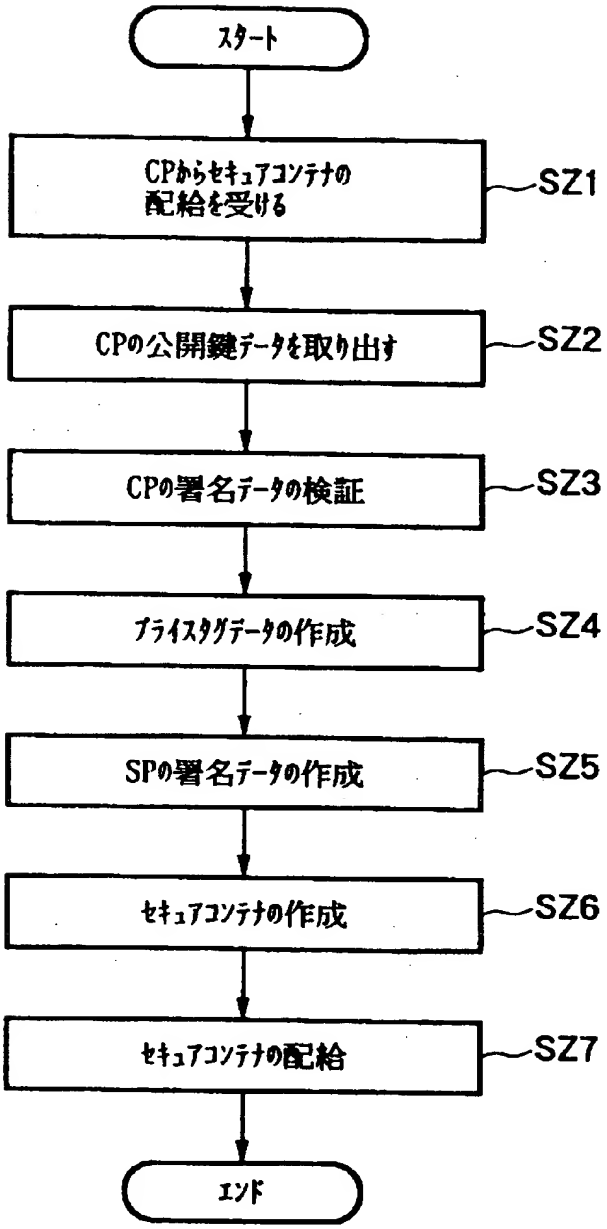
【図５０】


301 コンテンツプロバイダ
111 コンテンツマスターソースサーバ
112 電子透かし情報付加部
113 圧縮部
114 暗号化部 (Kc)
115 乱数発生部
116 暗号化部 (KD1～KD6)
118 セキュアコンテナ作成部
118a セキュアコンテナデータベース
119 記憶部 (データベース)
120 相互認証部
121 暗号化・復号部 (KSES)
122 権利書データ作成部
117 署名処理部 (KCP,S)
125 EMDサービスセンタ管理部
324 サービスプロバイダ管理部 (通信ゲートウェイ)
104
S111
S112
S113
Kc
C,Meta,Soft
Kc
KD1～KD6
SDC1～SDC3
CERCP
SIG1,ESC
Kc
106
SDC1～SDC3
Mod1
Meta,Soft
CERCP,STG1,ESC
104 セキュアコンテナ
KSES
106 権利書データ

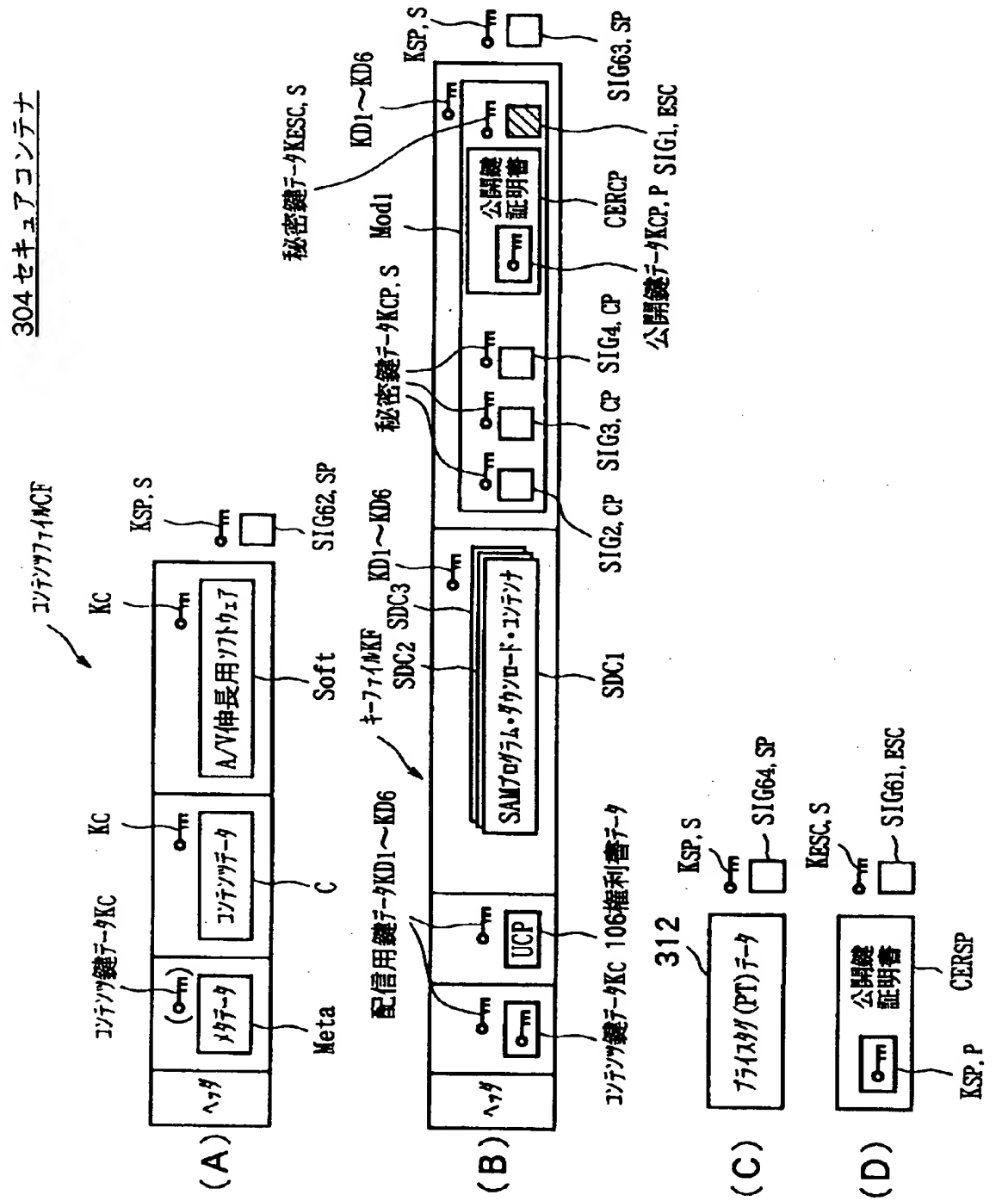
【図５１】


310サービスプロバイダ
CF, KF, CERSP&SIG61, ESC
304, 900
309
ユーザホーム
ネットワーク管理部
(通信ゲートウェイ)
357
309
CP用購入履歴データ
900 ユーザ嗜好
フィルタデータ
920
ユーザ嗜好
フィルタ生成部
358
EMDサービスセンタ
管理部
304
355
セキュアコンテナ
作成部
355a
309
記憶部
351
312プライスタグデータ
104
350
コンテンツプロバイダ
管理部
104
354
署名処理部
356
プライスタグデータ
作成部
暗号化・復号部
(KSES)
353
KSES
相互認証部
352

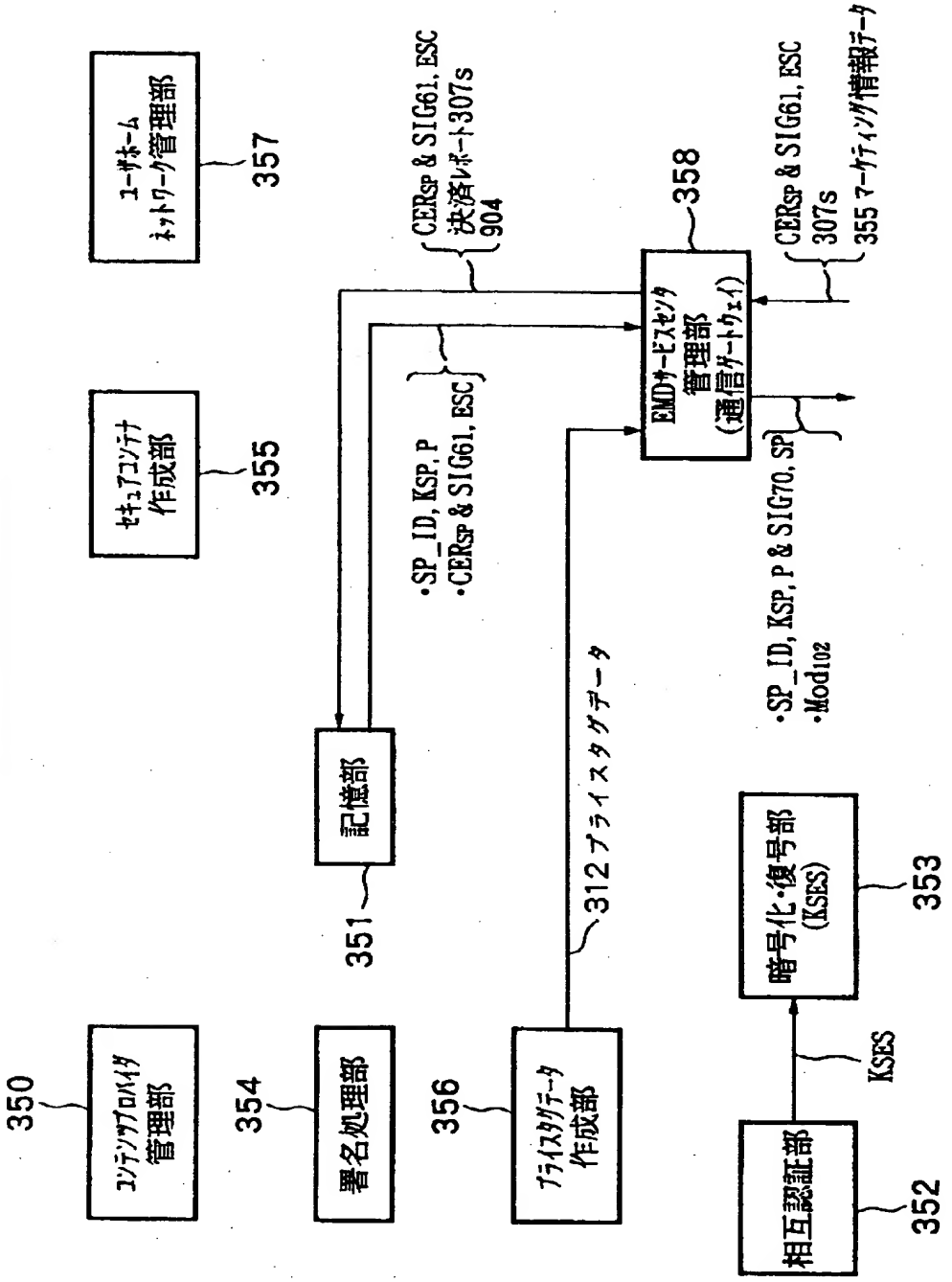
【図５２】


スタート
CPからセキュアコンテナの配給を受ける
SZ1
CPの公開鍵データを取り出す
SZ2
CPの署名データの検証
SZ3
プライスタグデータの作成
SZ4
SPの署名データの作成
SZ5
セキュアコンテナの作成
SZ6
セキュアコンテナの配給
SZ7
エンド

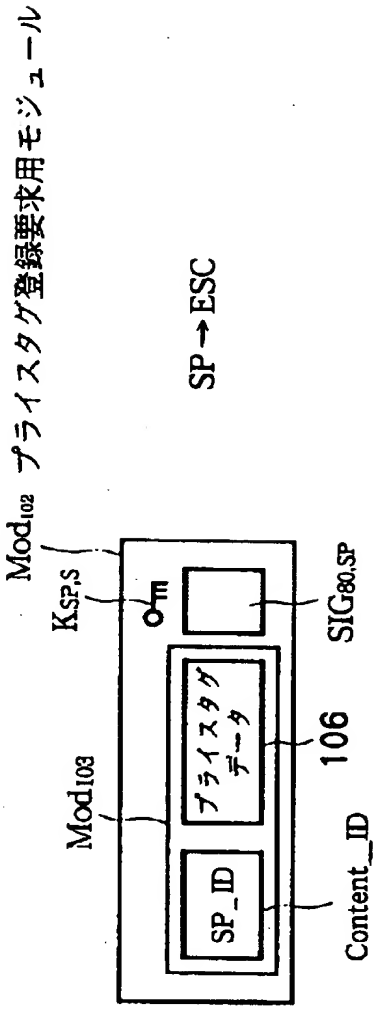
【図５３】


304 セキュアコンテナ
コンテンツファイルCF
Kc
KSP, S
A/V伸長用ソフトウェア
Soft
SIG62, SP
コンテンツ鍵データKc
コンテンツデータ
C
メタデータ
Meta
ヘッダ
(A)
秘密鍵データKESC, S
KD1～KD6
KSP, S
Mod1
公開鍵証明書
CERCP
SIG63, SP
公開鍵データKCP, P
SIG1, ESC
秘密鍵データKCP, S
SIG4, CP
SIG3, CP
SIG2, CP
キーファイルKF
SDC2
SDC3
KD1～KD6
SAMプログラム・ダウンロード・コンテンツ
SDC1
配信用鍵データKD1～KD6
UCP
コンテンツ鍵データKc
106権利書データ
ヘッダ
(B)
312
KSP, S
SIG64, SP
プライスタグ(PT)データ
(C)
KESC, S
SIG61, ESC
公開鍵証明書
CERSP
KSP, P
(D)

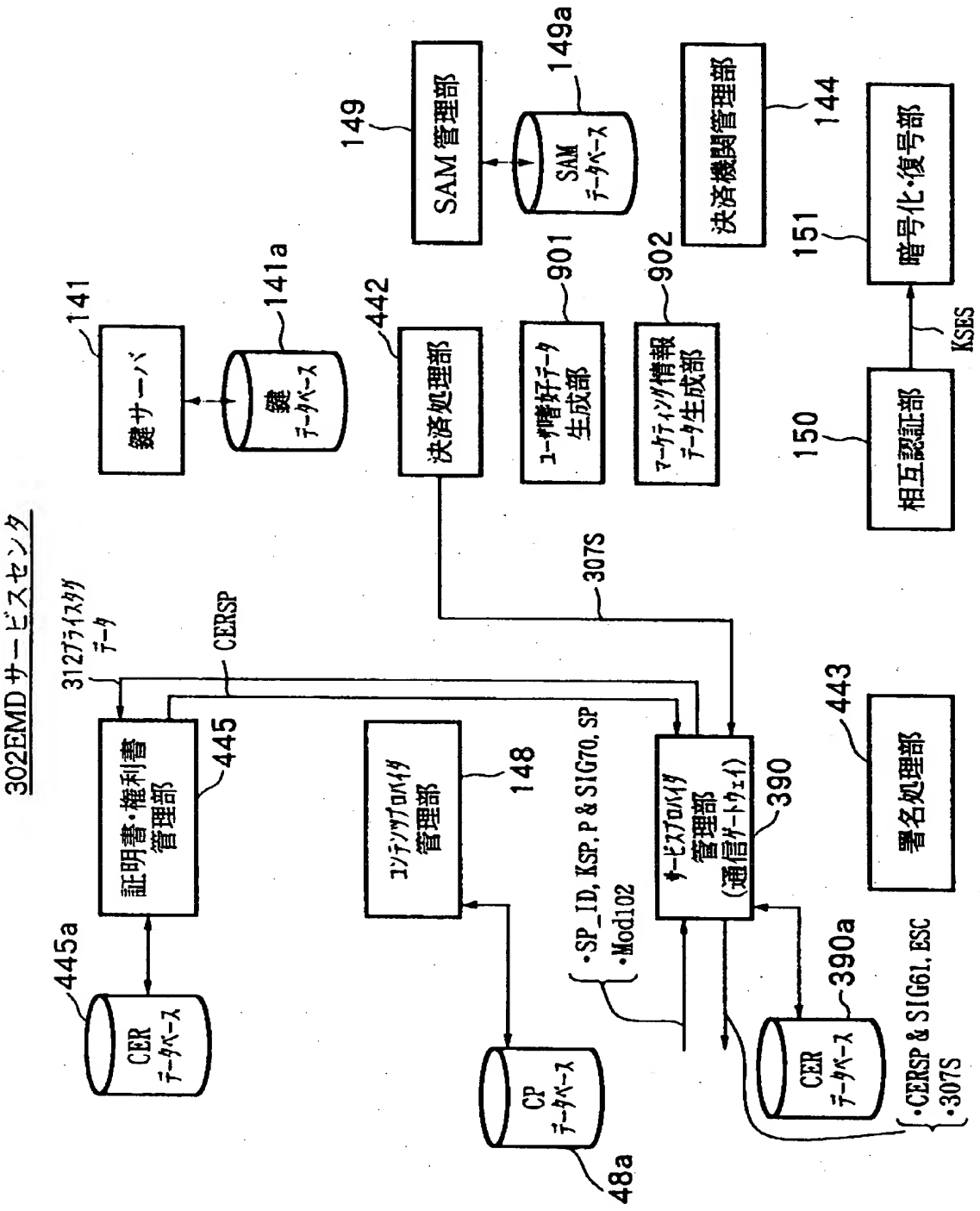
【図５４】


310サービスプロバイダ
350
コンテンツプロバイダ管理部
354
署名処理部
356
プライスタグデータ作成部
351
記憶部
355
セキュアコンテナ作成部
357
ユーザホーム ネットワーク管理部
358
EMDサービスセンタ管理部（通信ゲートウェイ）
353
暗号化・復号部（KSES）
352
相互認証部
KSES
312プライスタグデータ
•SP_ID, KSP, P
•CERSP & SIG61, ESC
CERSP & SIG61, ESC 決済レポート307s 904
•SP_ID, KSP, P & SIG70, SP
•Mod102
CERSP & SIG61, ESC 307s 355マーケティング情報データ

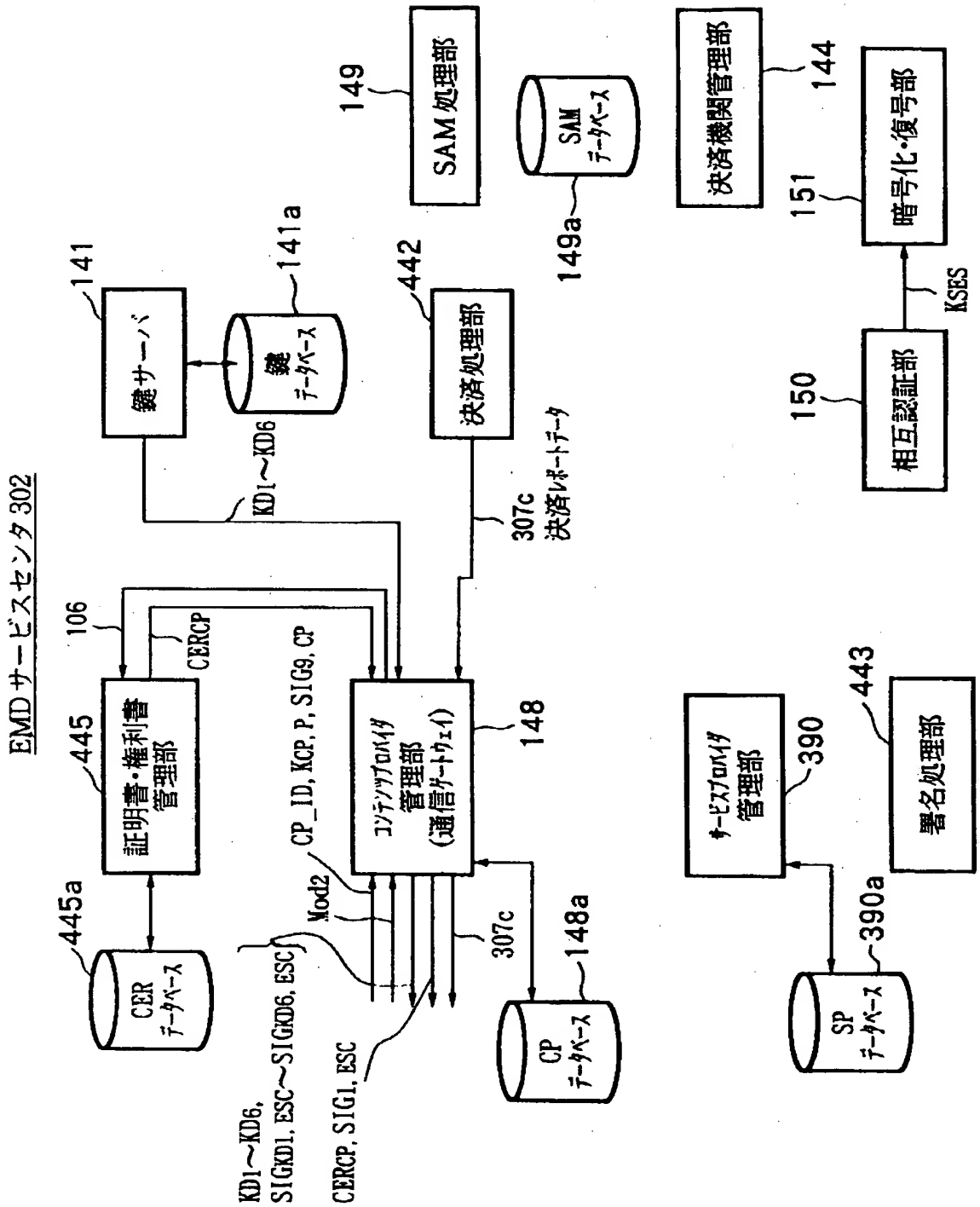
【図５５】


プライスタグ登録要求用モジュール
SP→ESC
Mod102
KSP,S
SIG80,SP
Mod103
プライスタグデータ
106
SP_ID
Content_ID

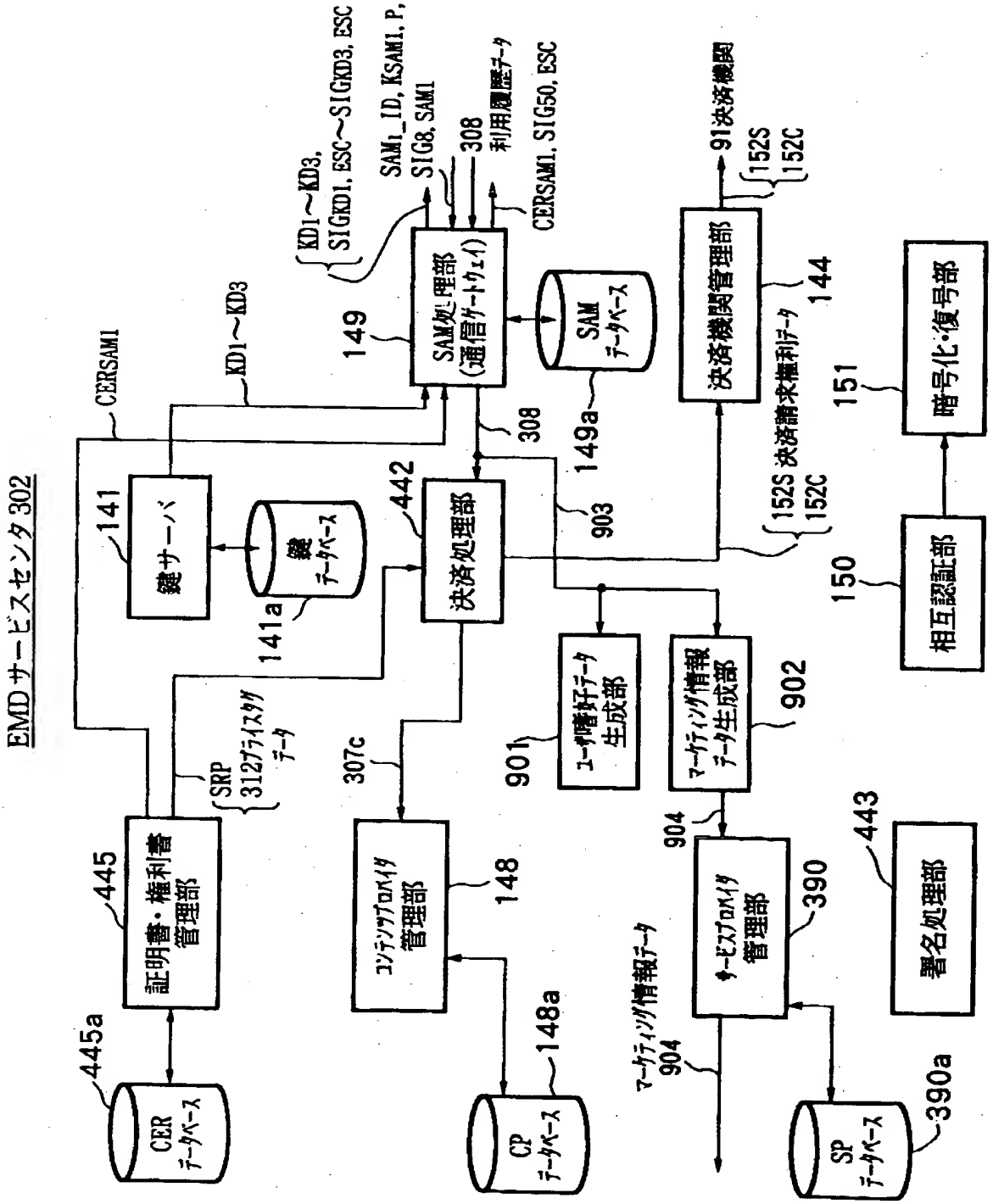
【図５６】


302EMDサービスセンタ
141
鍵サーバ
141a
鍵データベース
149
SAM管理部
149a
SAMデータベース
442
決済処理部
901
ユーザ嗜好データ生成部
902
マーケティング情報データ生成部
144
決済機関管理部
151
暗号化・復号部
150
相互認証部
KSES
307S
312プライスタグデータ
CERSP
445
証明書・権利書管理部
445a
CERデータベース
148
コンテンツプロバイダ管理部
148a
CPデータベース
390
サービスプロバイダ管理部（通信ゲートウェイ）
390a
CERデータベース
443
署名処理部
・SP_ID, KSP, P & SIG70, SP
・Mod102
・CERSP & SIG61, ESC
・307S

【図５７】


EMDサービスセンタ302
鍵サーバ
141
鍵 データベース
141a
KD1～KD6
SAM処理部
149
SAM データベース
149a
決済処理部
442
307c 決済レポートデータ
決済機関管理部
144
暗号化・復号部
151
KSES
相互認証部
150
106
CERCP
証明書・権利書管理部
445
CER データベース
445a
CP_ID, KCP, P, SIG9, CP
Mod2
コンテンツプロバイダ管理部（通信ゲートウェイ）
148
307c
CP データベース
148a
KD1～KD6, SIGKD1, ESC～SIGKD6, ESC
CERCP, SIG1, ESC
サービスプロバイダ管理部
390
署名処理部
443
SP データベース
390a

【図５８】

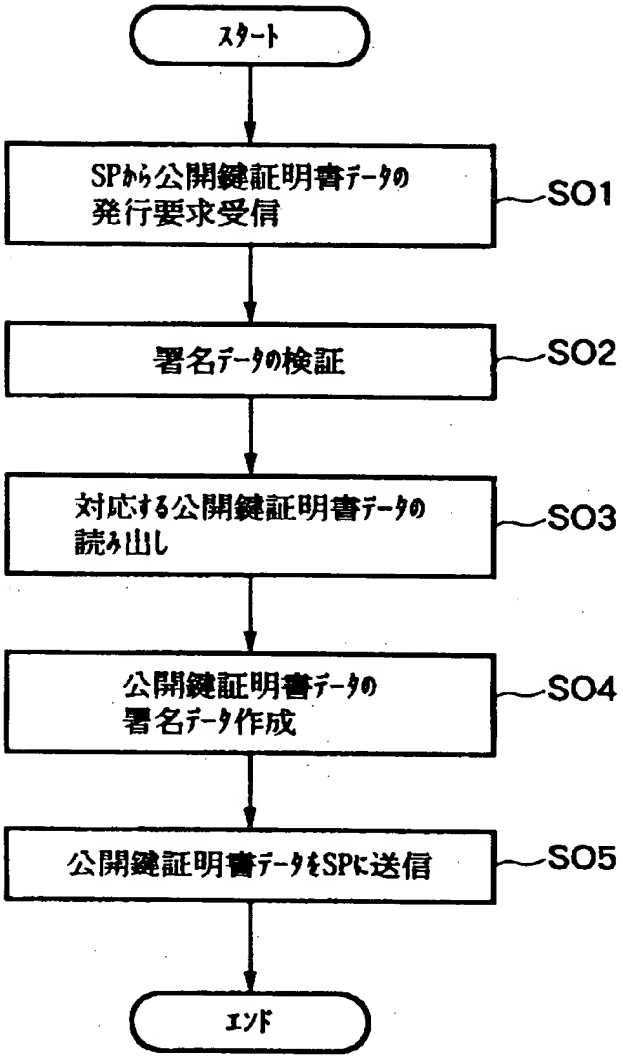

EMDサービスセンタ302
CERSAM1
KD1～KD3
KD1～KD3,
SIGKD1, ESC～SIGKD3, ESC
SAM1_ID, KSAM1, P,
SIG8, SAM1
308
利用履歴データ
CERSAM1, SIG50, ESC
91決済機関
152S
152C
149
SAM処理部
(通信ゲートウェイ)
SAM
データベース
決済機関管理部
144
151
暗号化・復号部
141
鍵サーバ
鍵
データベース
141a
442
決済処理部
308
149a
903
152S 決済請求権利データ
152C
150
相互認証部
SRP
312プライスタグ
データ
307c
901
ユーザ嗜好データ
生成部
マーケティング情報
データ生成部
902
445
証明書・権利書
管理部
コンテンツプロバイダ
管理部
148
904
サービスプロバイダ
管理部
390
443
署名処理部
マーケティング情報データ
904
445a
CER
データベース
148a
CP
データベース
390a
SP
データベース

【図５９】

利用履歴データ308の内容

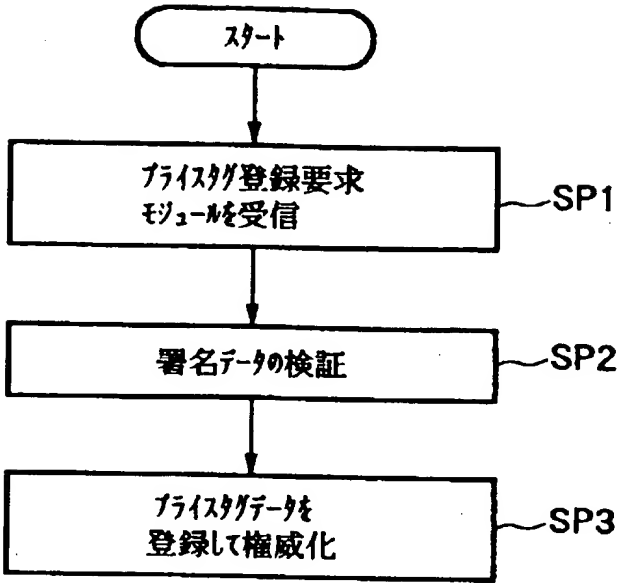
識別子Content__ID
識別子CP__ID
識別子SP__ID
コンテンツデータCの信号諸元データ
コンテンツデータCの圧縮方法
記録媒体の識別子Media_ ID
識別子SAM__ID、
ユーザのUSER__ID

【図６０】



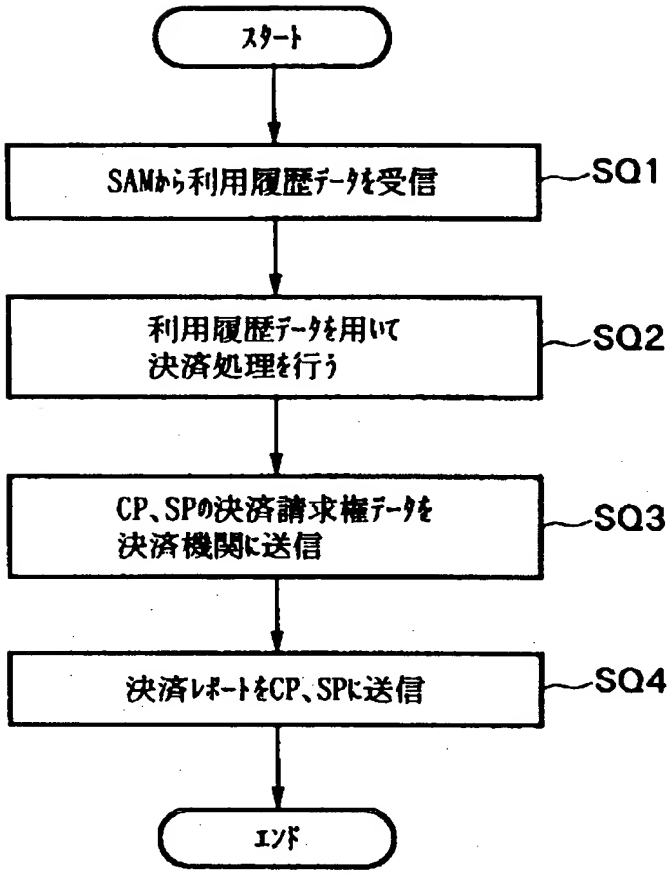
SPからの公開鍵証明書データの発行要求に応じたESCの処理

【図６１】



ESCにおけるプライスタグデータの登録処理

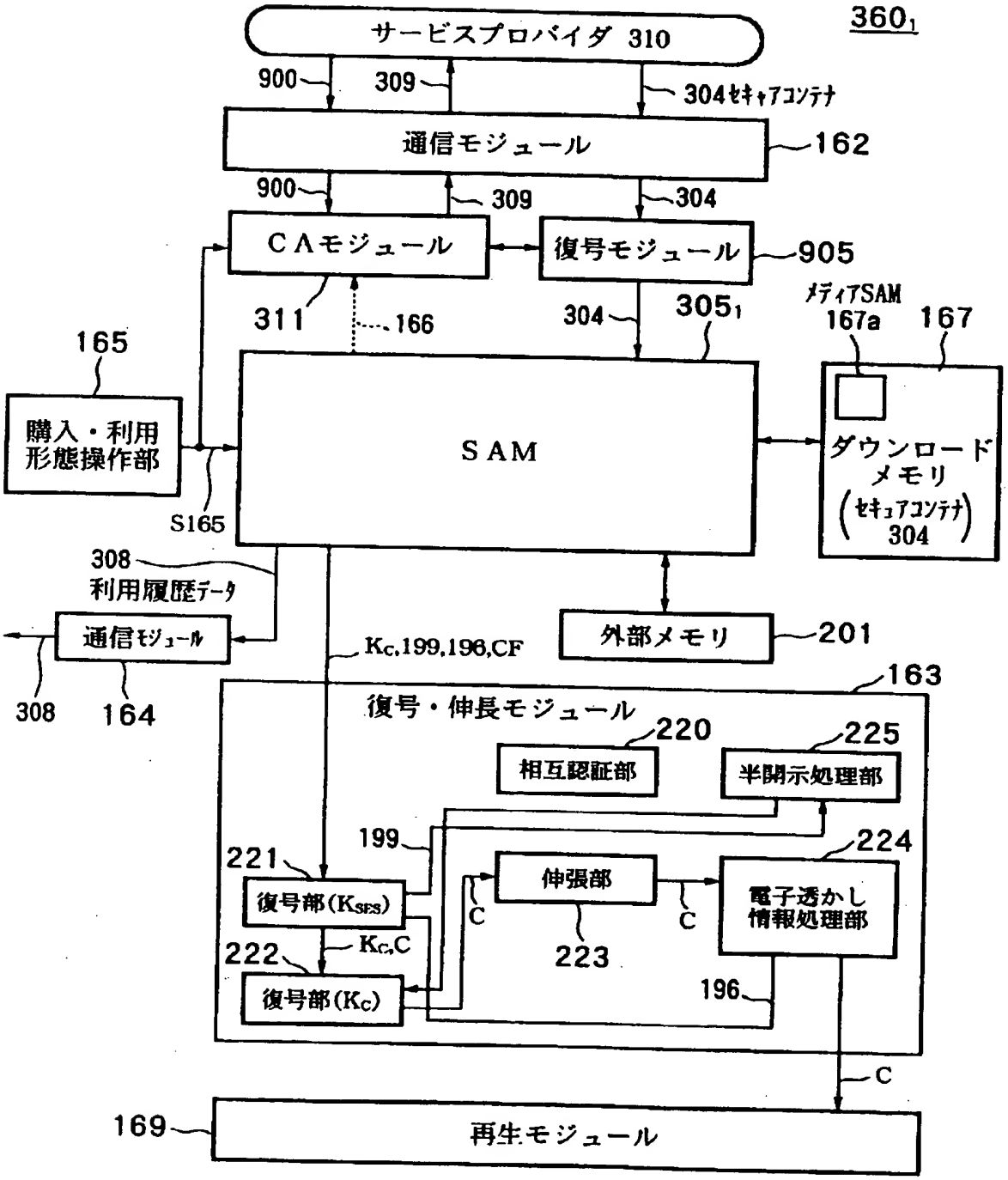
【図６２】



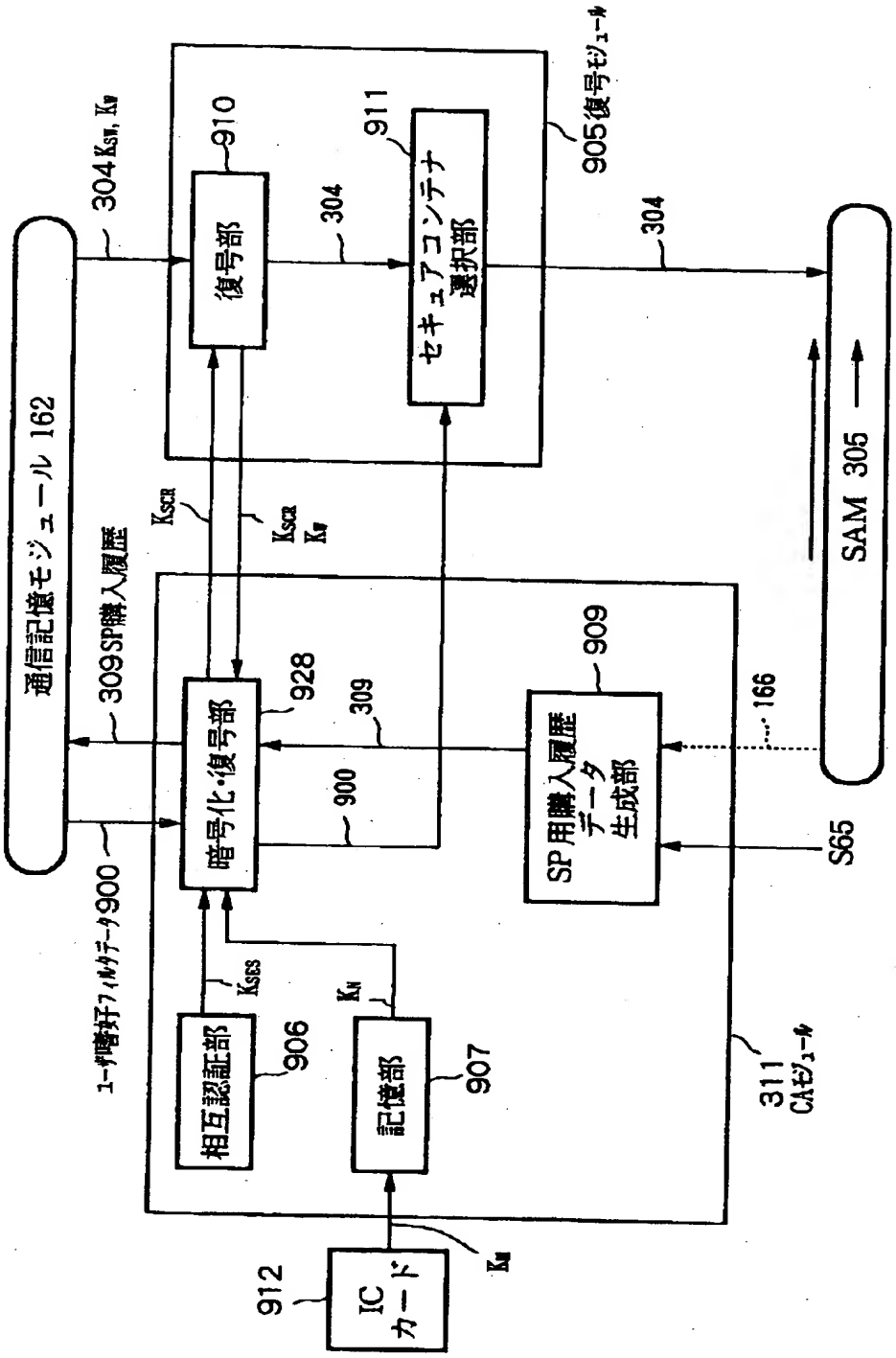
ESCにおける決済処理

出証特２０００－３０４３０２６

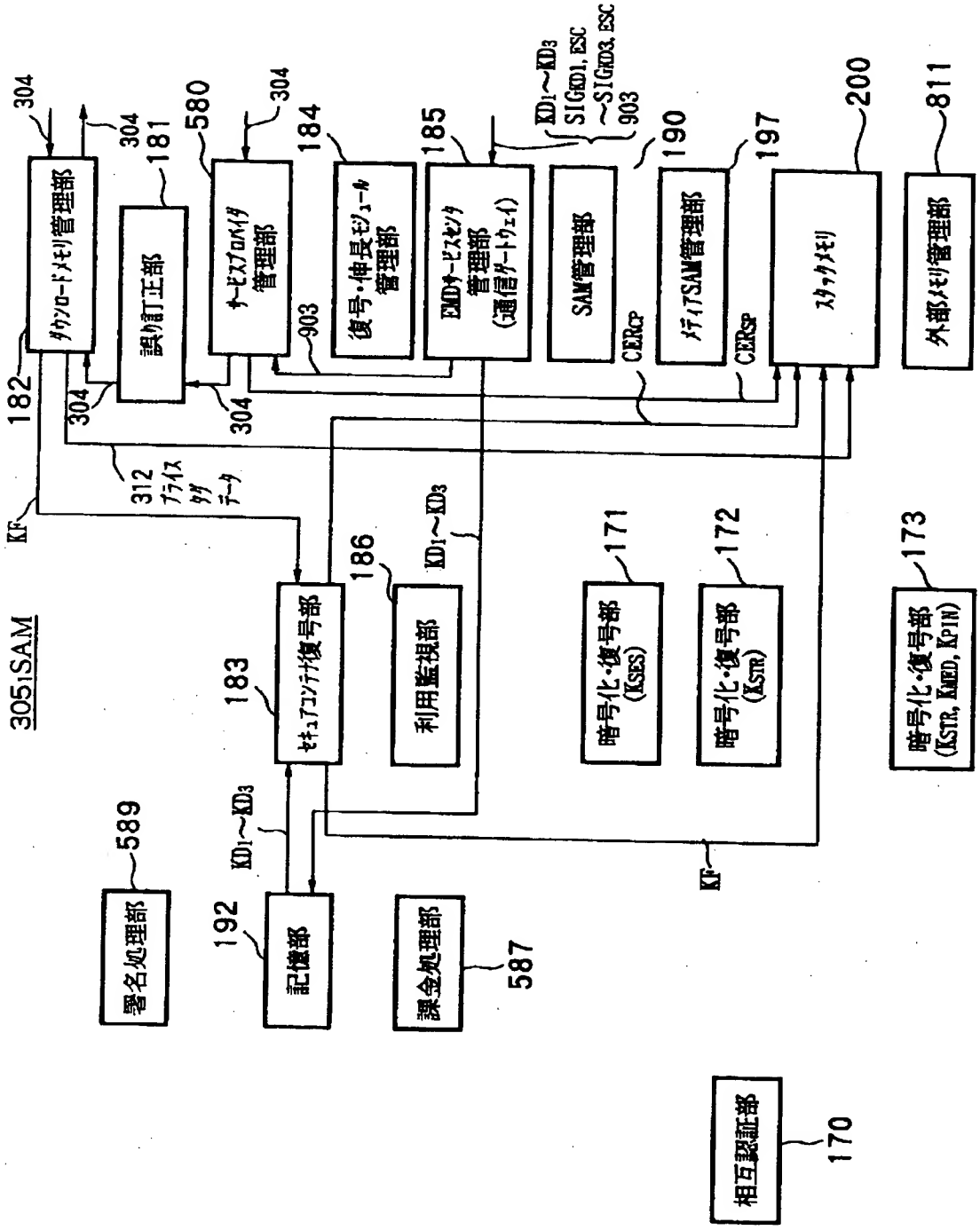
【図６３】


サービスプロバイダ 310
360₁
900
309
304セキュアコンテナ
通信モジュール
162
900
309
304
CAモジュール
復号モジュール
905
311
166
304
305₁
メディアSAM
167a
167
165
購入・利用
形態操作部
SAM
ダウンロード
メモリ
(セキュアコンテナ)
304
S165
308
利用履歴データ
通信モジュール
Kc,199,196,CF
外部メモリ
201
163
308
164
復号・伸長モジュール
220
相互認証部
225
半開示処理部
199
224
221
伸張部
電子透かし
情報処理部
復号部(KSES)
C
C
Kc,C
222
223
復号部(Kc)
196
C
169
再生モジュール

【図６４】


通信記憶モジュール 162
304 K_{SM}, K_M
復号部
910
304
セキュアコンテナ選択部
911
905復号モジュール
304
SAM 305
K_{SCR}
K_{SCR} K_M
309SP購入履歴
暗号化・復号部
928
309
SP用購入履歴データ生成部
909
166
900
S65
ユーザ嗜好フィルタデータ900
K_{SES}
K_M
相互認証部
906
記憶部
907
311 CAモジュール
912
ICカード
K_M

【図６５】

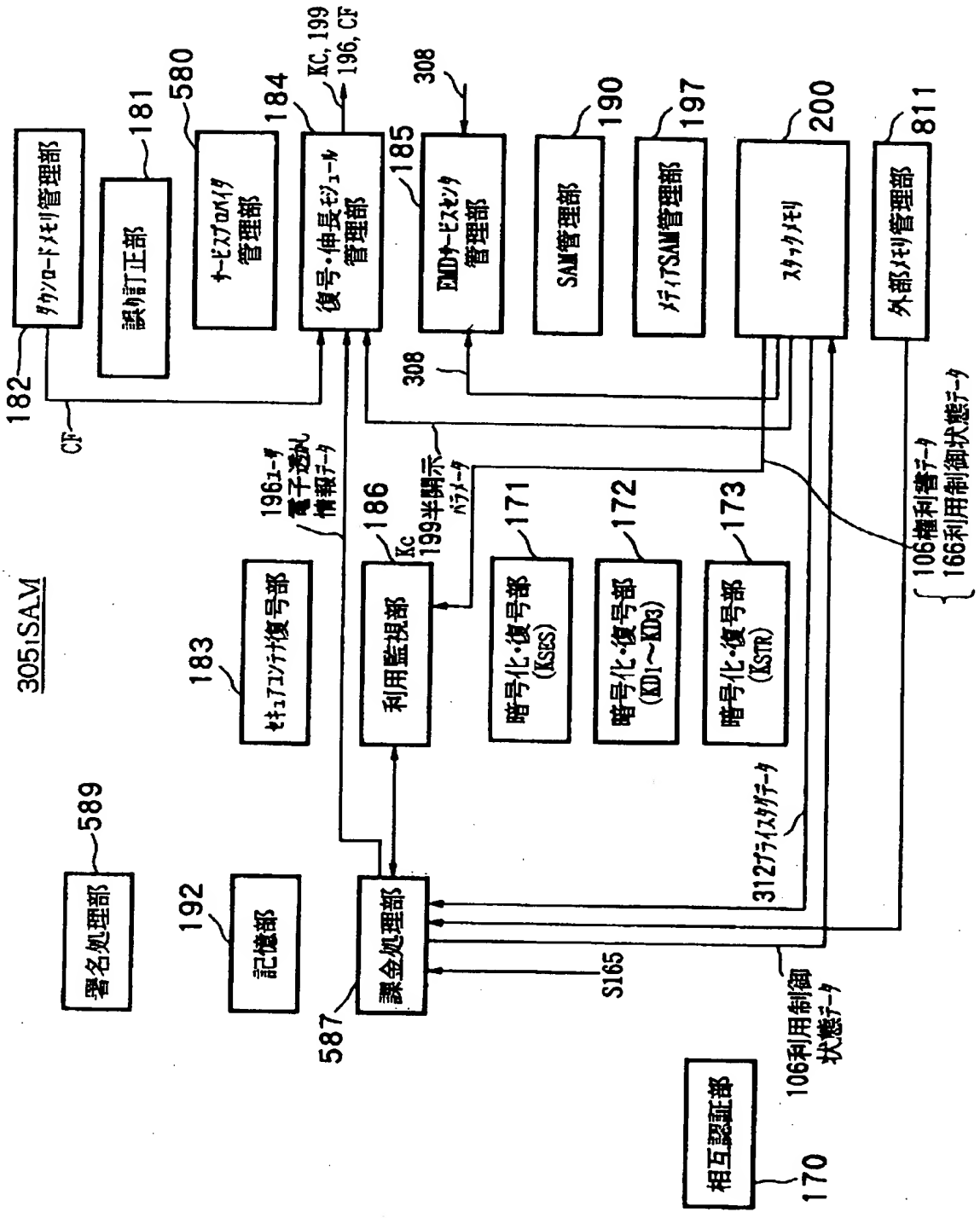

305₁SAM
304
181
580
184
185
190
197
200
811
182
312
ﾌﾗｲｽ
ﾀｸﾞﾃﾞｰﾀ
KF
183
186
171
172
173
589
192
587
170
KD₁～KD₃
SIGKD1, ESC
～SIGKD3, ESC
903
CERCP
CERSP
ﾀﾞｳﾝﾛｰﾄﾞﾒﾓﾘ管理部
誤り訂正部
ｻｰﾋﾞｽﾌﾛｸﾞﾗﾑ管理部
復号・伸長ﾓｼﾞｭｰﾙ管理部
EMDｻｰﾋﾞｽｾﾝﾀ管理部（通信ｹﾞｰﾄｳｪｲ）
SAM管理部
ﾒﾃﾞｨｱSAM管理部
ﾌﾗｯｼｭﾒﾓﾘ
外部ﾒﾓﾘ管理部
ｾｷｭﾘﾃｨｺﾝﾃﾝﾂ復号部
利用監視部
暗号化・復号部（KSES）
暗号化・復号部（KSTR）
暗号化・復号部（KSTR, KMED, KPIN）
署名処理部
記憶部
課金処理部
相互認証部

【図６６】

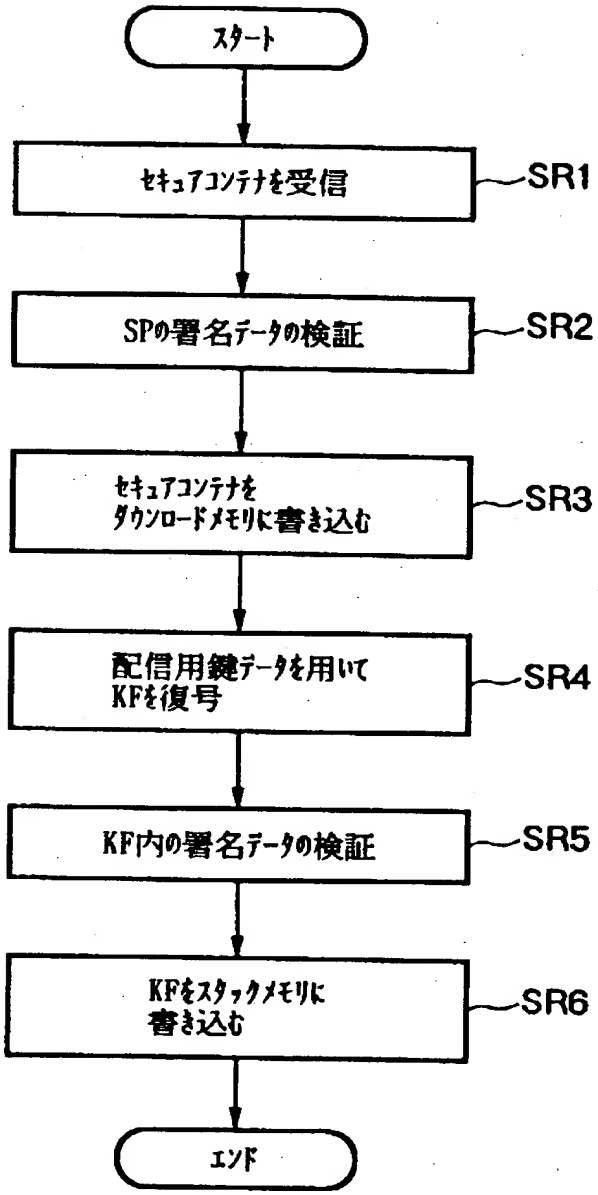
スタックメモリ200の記憶データ

コンテンツ鍵データ K_C
権利書データ（UCP）106
不揮発性メモリ201のロック鍵データ K_{LOC}
コンテンツプロバイダ301の公開鍵証明書データ CER_{CP}
サービスプロバイダ301の公開鍵証明書データ CER_{SP}
利用制御情状態データ（UCS）166
SAMプログラム・ダウンロード・コンテナ SD_1～SDC_3
プライスタグデータ312

【図６７】

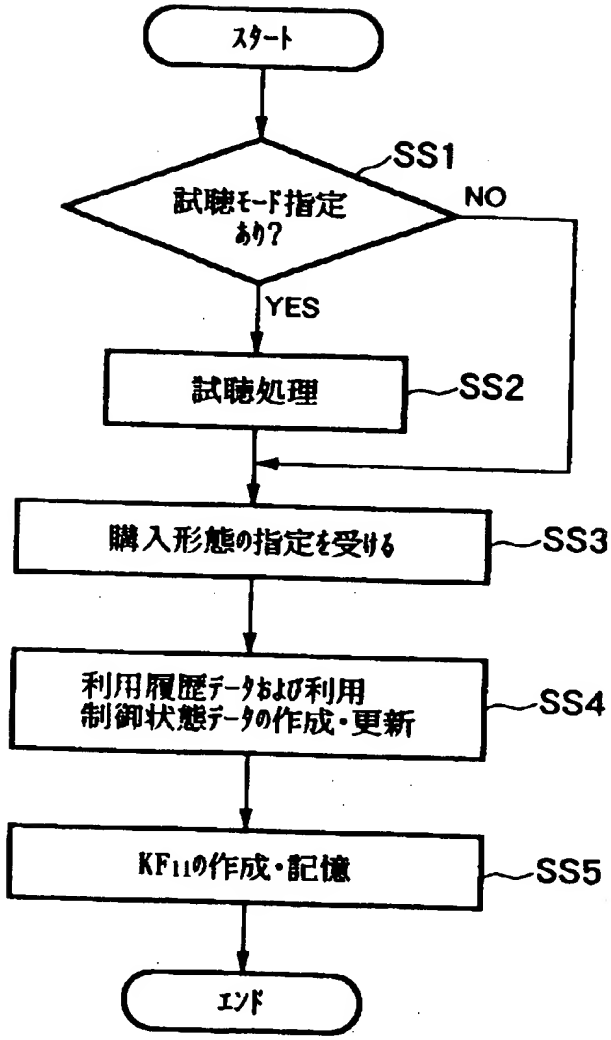

305:SAM
182
CF
181
誤り訂正部
580
サービスコントロール管理部
184
Kc, 199
196, CF
復号・伸長モジュール管理部
185
308
EMDサービスセンタ管理部
190
SAM管理部
197
メディアSAM管理部
200
スタックメモリ
811
外部メモリ管理部
308
196ユーザ電子透かし情報データ
186
Kc
199半開示パラメータ
183
セキュアコンテナ復号部
利用監視部
171
暗号化・復号部 (KSES)
172
暗号化・復号部 (KD1～KD3)
173
暗号化・復号部 (KSTR)
106権利書データ
166利用制御状態データ
589
署名処理部
192
記憶部
587
課金処理部
312ライスカウンタデータ
S165
106利用制御状態データ
相互認証部
170

【図６８】



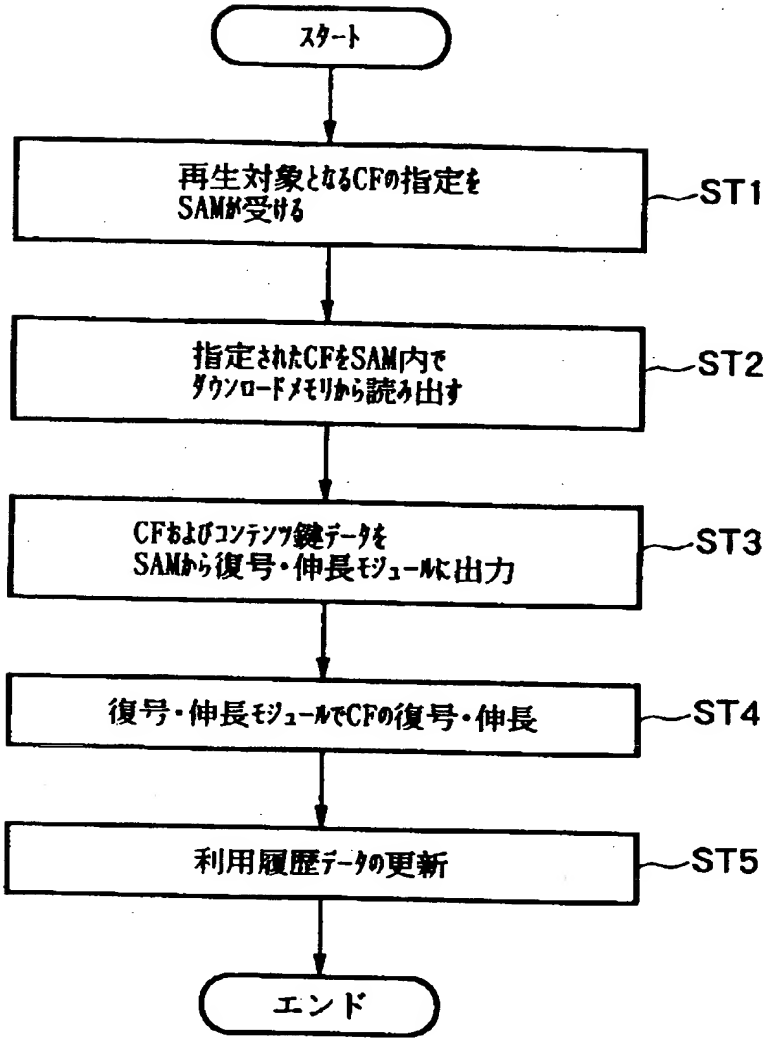
SAMにおけるKFの復号処理

【図６９】



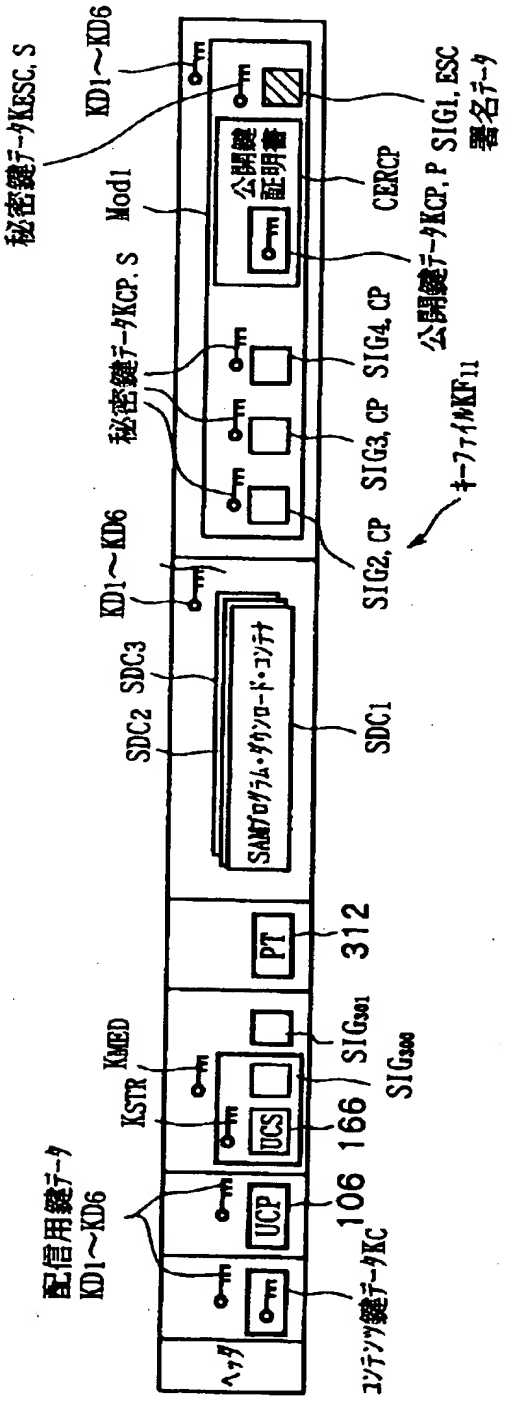
SAMにおけるセキュアコンテナの購入形態決定処理

【図７０】

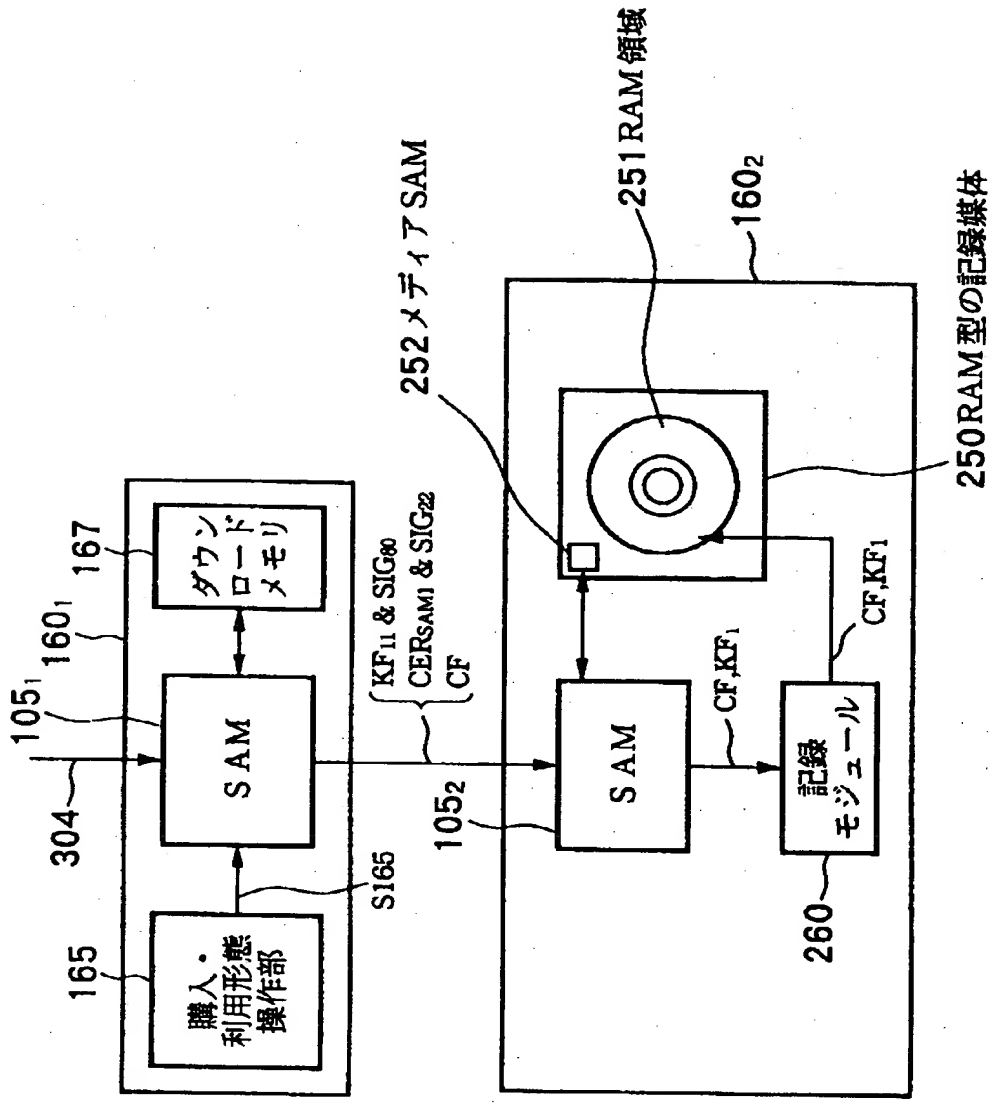


コンテンツデータの再生処理

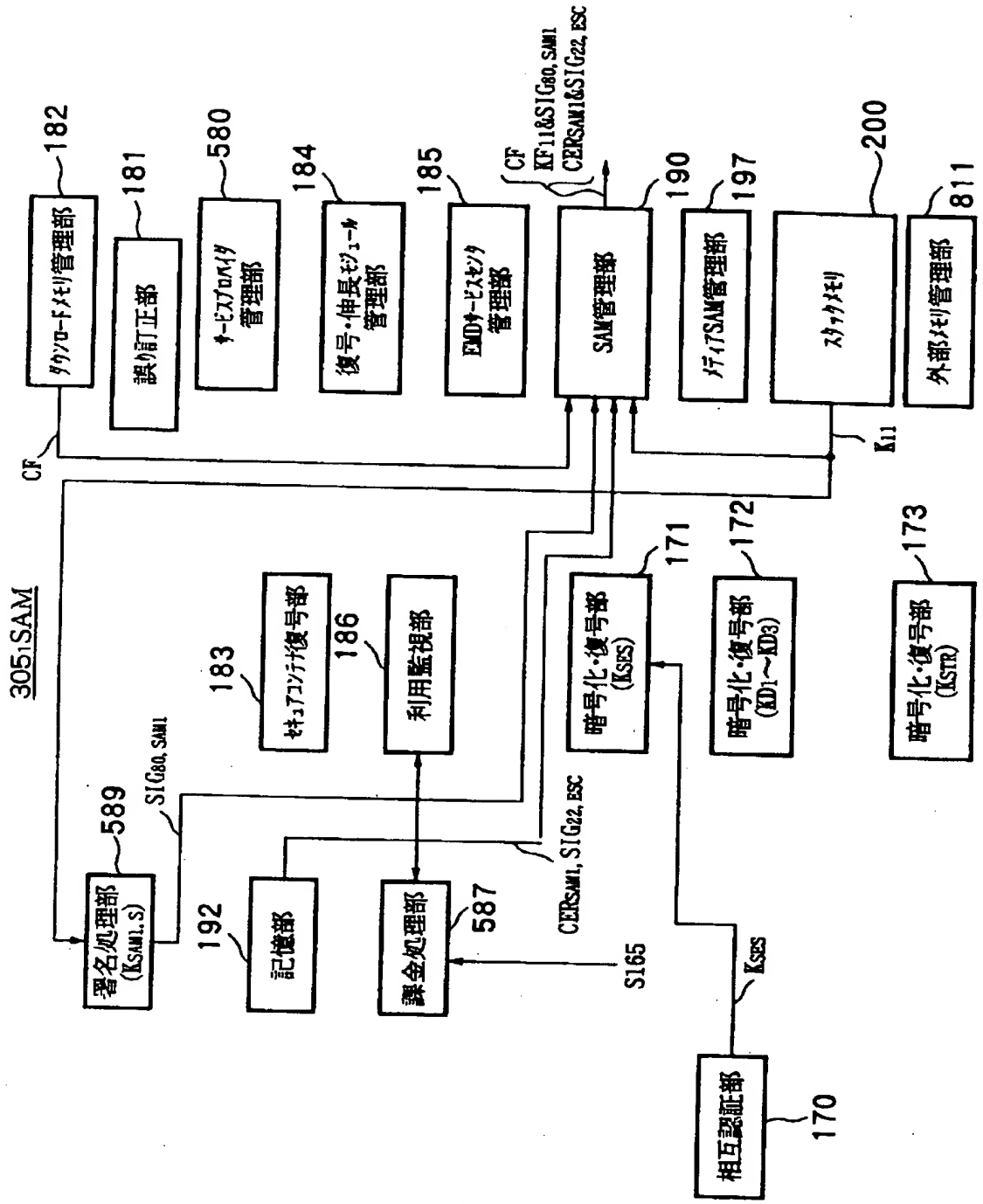
【図７１】


秘密鍵データKESC, S
KD1～KD6
Mod1
秘密鍵データKCP, S
KD1～KD6
SDC3
SDC2
SDC1
SIG2, CP
SIG3, CP
SIG4, CP
CERCP
公開鍵データKCP, P
SIG1, ESC
署名データ
キーファイルKF11
PT
312
KMED
KSTR
UCS
UCP
106
166
SIG301
SIG300
配信用鍵データ
KD1～KD6
コンテンツ鍵データKC
ヘッダ

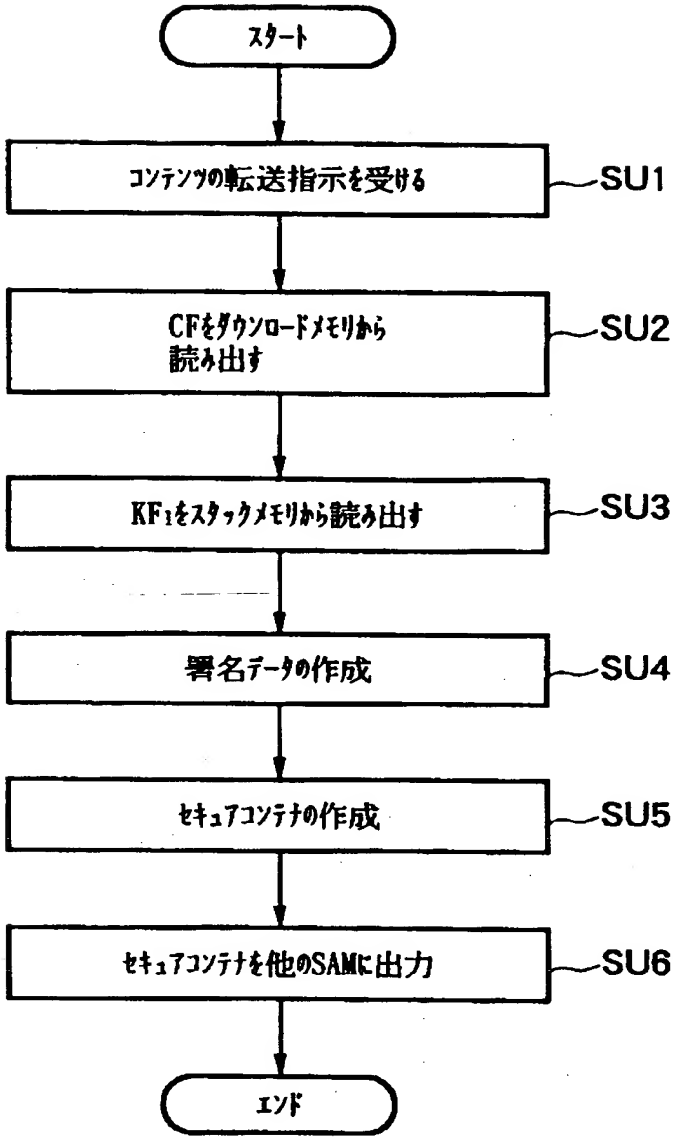
【図７２】


250RAM型の記録媒体
251RAM領域
160₂
252メディアSAM
167
ダウンロードメモリ
160₁
105₁
304
SAM
165
購入・利用形態操作部
S165
KF₁₁ & SIG₀₀
CERSAM1 & SIG₂₂
CF
105₂
SAM
CF,KF₁
CF,KF₁
記録モジュール
260

【図７３】

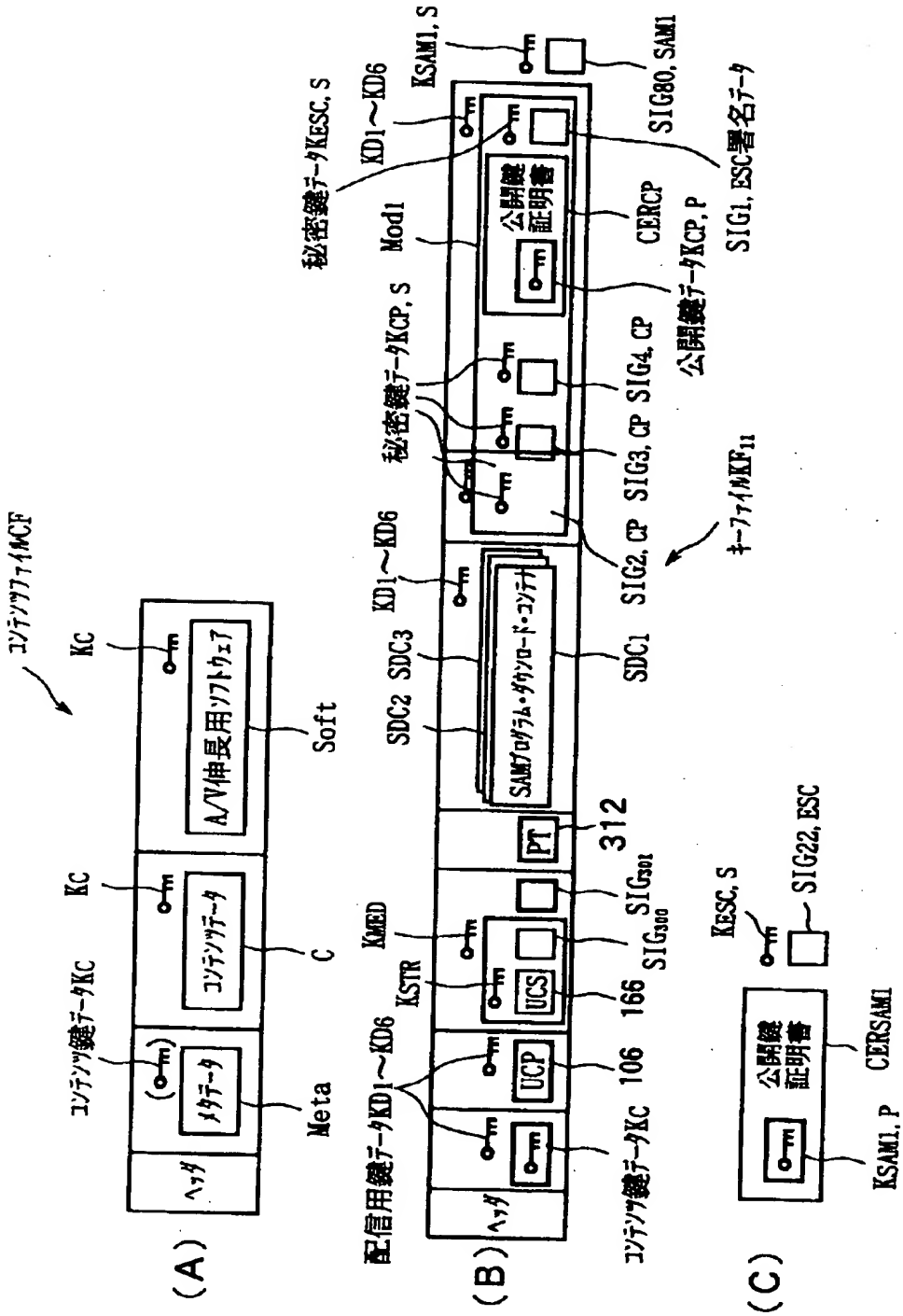

305 SAM
182
181
580
184
185
190
197
200
811
CF
KF11&SIG60, SAM1
CERSAM1&SIG22, ESC
K11
183
186
171
172
173
589
587
192
S165
170
SIG60, SAM1
CERSAM1, SIG22, ESC
KSES
署名処理部
(KSAM1, S)
記憶部
課金処理部
利用監視部
暗号化・復号部
(KSES)
暗号化・復号部
(KD1～KD3)
暗号化・復号部
(KSTR)
相互認証部
SAM管理部
外部メモリ管理部

【図７４】

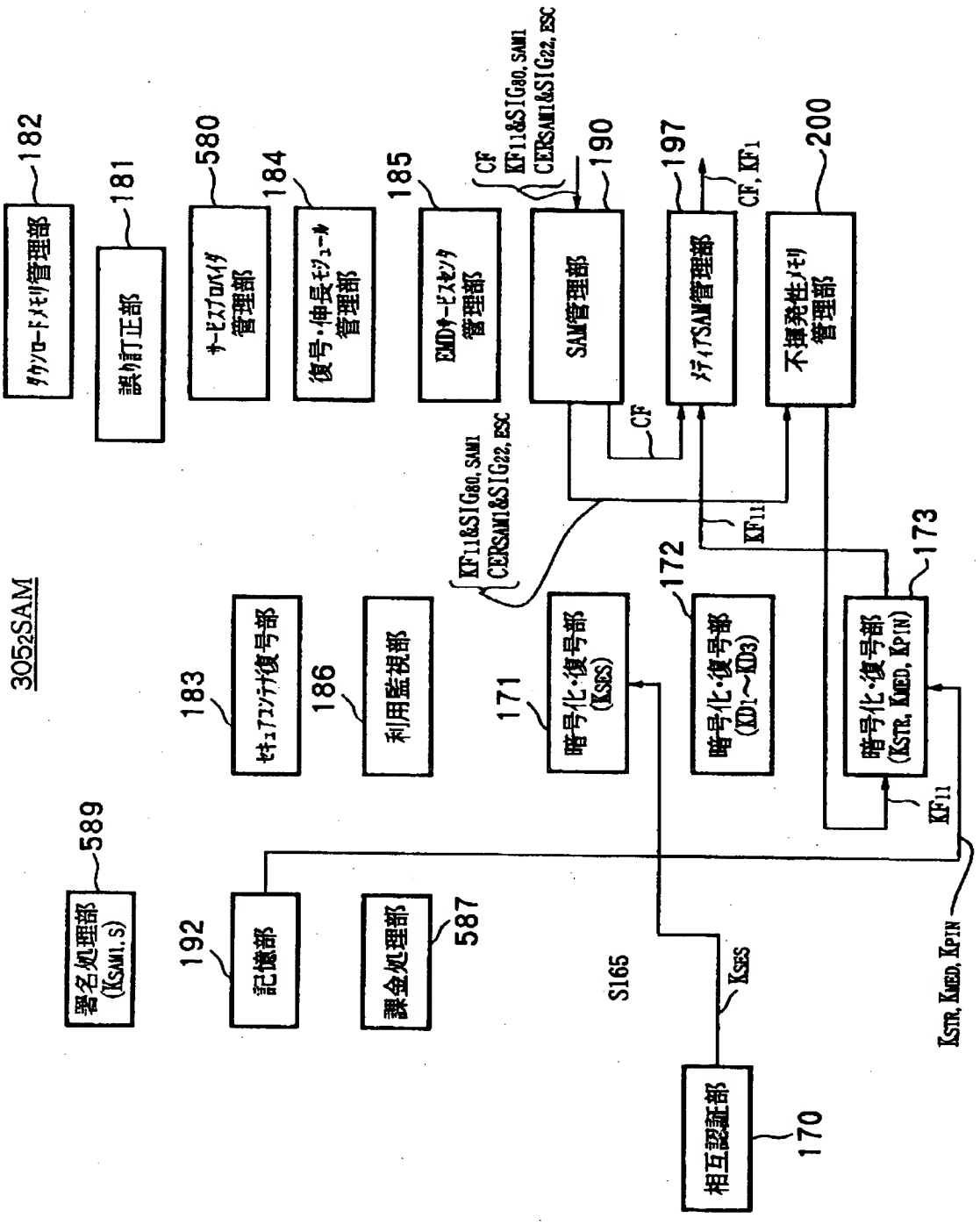


購入形態決定後のコンテンツを他のSAMに転送するSAMの処理

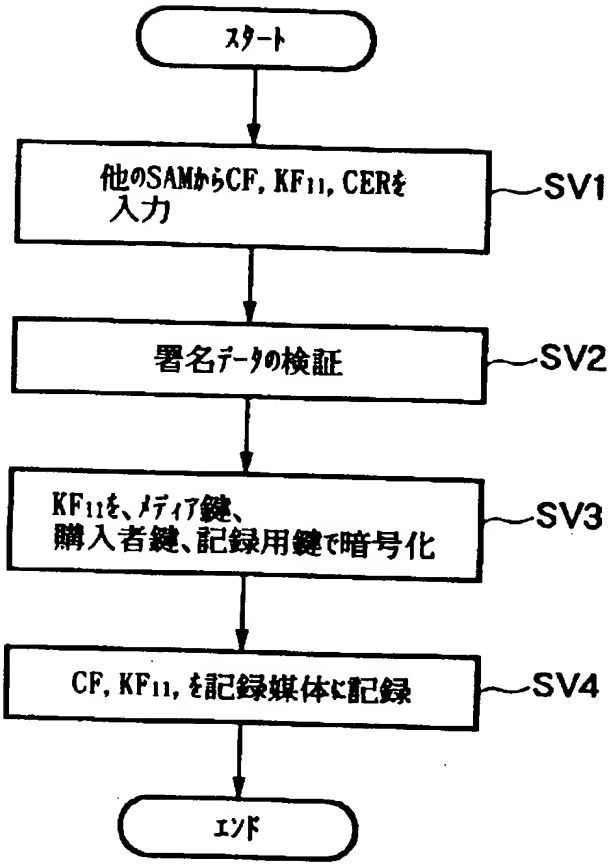
【図７５】


コンテンツファイルCF
Kc
A/V伸長用ソフトウェア
Soft
コンテンツ鍵データKc
Kc
コンテンツデータ
C
メタデータ
Meta
ヘッダ
(A)
秘密鍵データKESC, S
KD1～KD6
KSAM1, S
SIG80, SAM1
Mod1
公開鍵証明書
CERCP
秘密鍵データKCP, S
公開鍵データKCP, P
SIG1, ESC署名データ
SIG4, CP
SIG3, CP
SIG2, CP
キーファイルKF11
KD1～KD6
SDC2 SDC3
SAMプログラム・ダウンロード・コンテンツ
SDC1
PT
312
KMED
KSTR
UCS
166
SIG300
SIG301
配信用鍵データKD1～KD6
UCP
106
コンテンツ鍵データKC
ヘッダ
(B)
KESC, S
SIG22, ESC
公開鍵証明書
CERSAM1
KSAM1, P
(C)

【図７６】

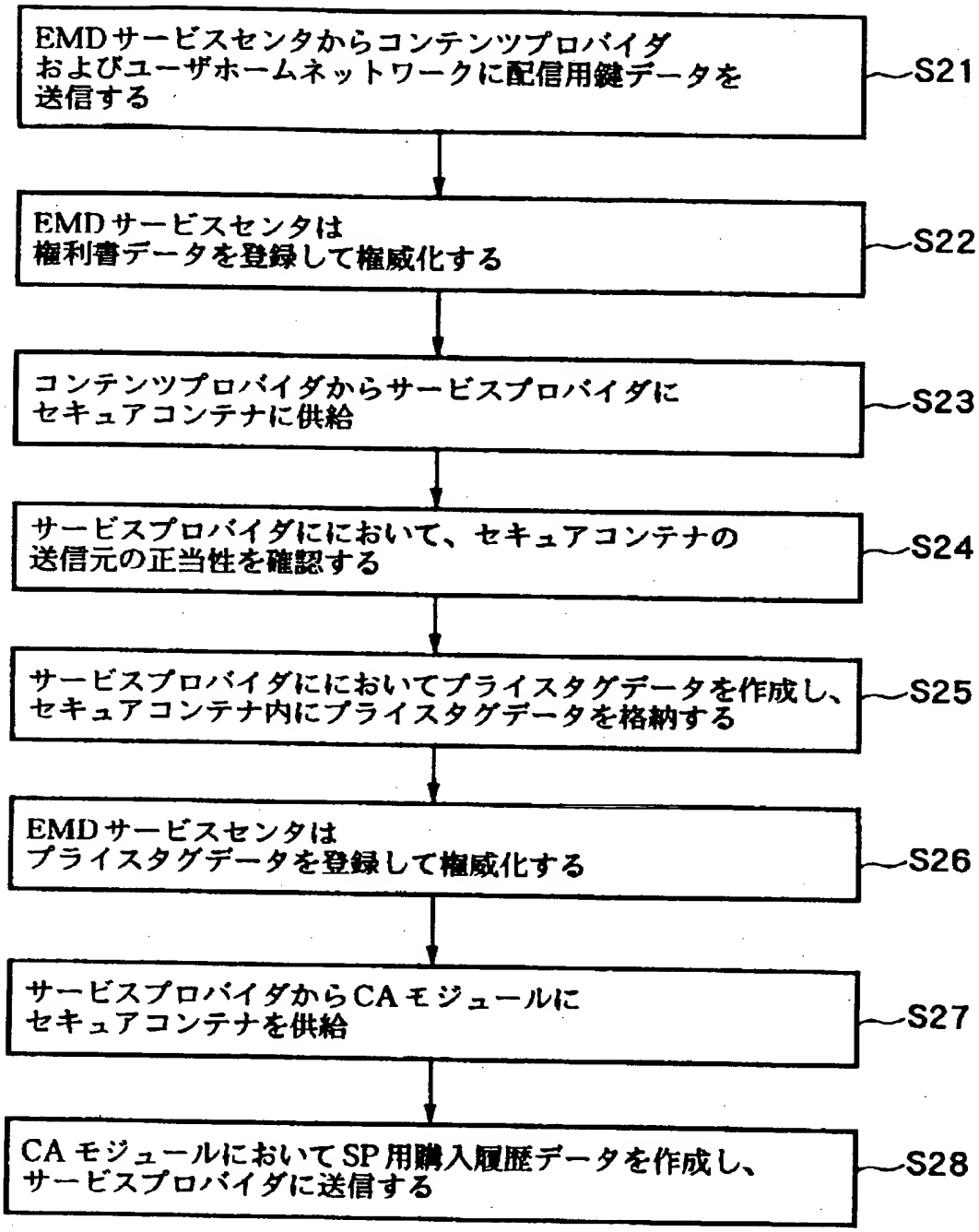

3052SAM
182
ダウンロードメモリ管理部
181
誤り訂正部
580
サービスプロバイダ管理部
184
復号・伸長モジュール管理部
185
EMDサービスセンタ管理部
CF
KF11&SIG80, SAM1
CERSAM1&SIG22, ESC
190
SAM管理部
197
メディアSAM管理部
CF, KF1
200
不揮発性メモリ管理部
KF11&SIG80, SAM1
CERSAM1&SIG22, ESC
CF
KF11
183
セキュアコンテナ復号部
186
利用監視部
171
暗号化・復号部 (KSES)
172
暗号化・復号部 (KD1～KD3)
173
暗号化・復号部 (KSTR, KMED, KPIN)
KF11
589
署名処理部 (KSAM1, S)
192
記憶部
587
課金処理部
S165
KSES
KSTR, KMED, KPIN
170
相互認証部

【図７７】

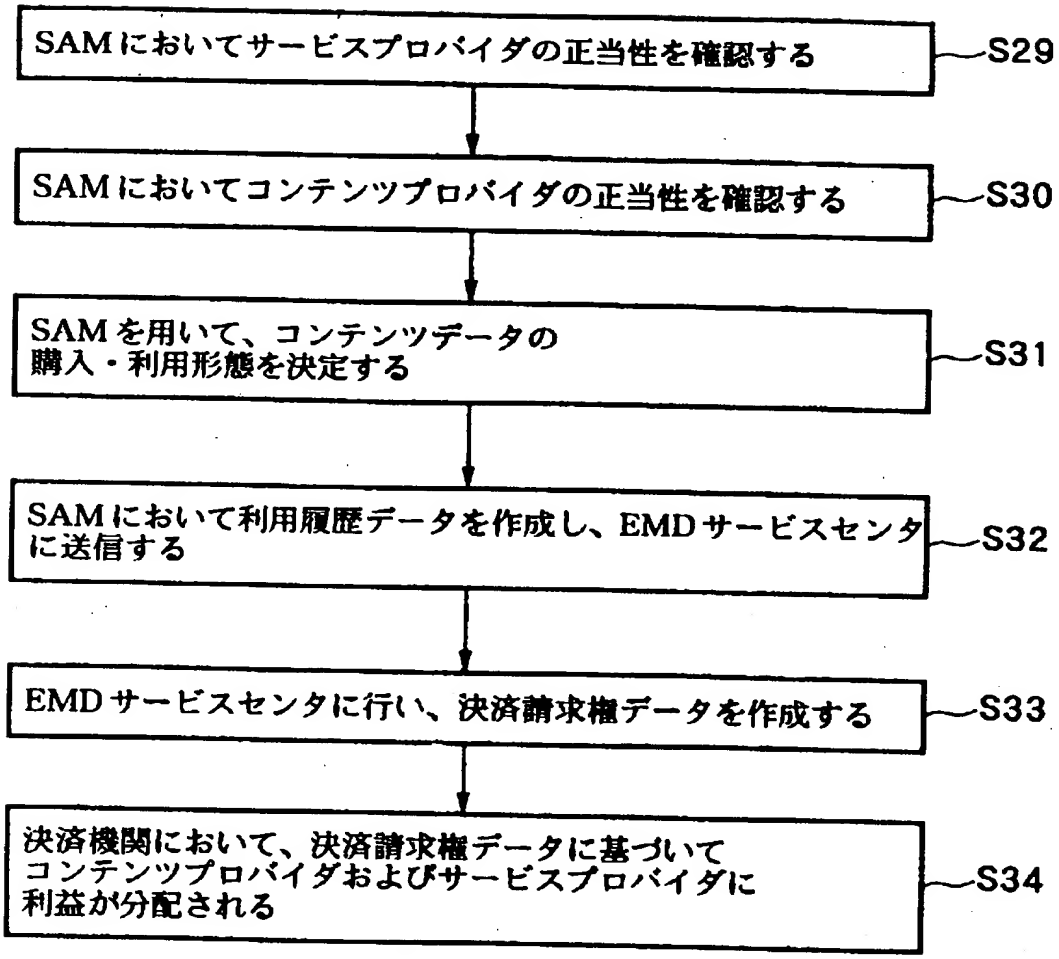


他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

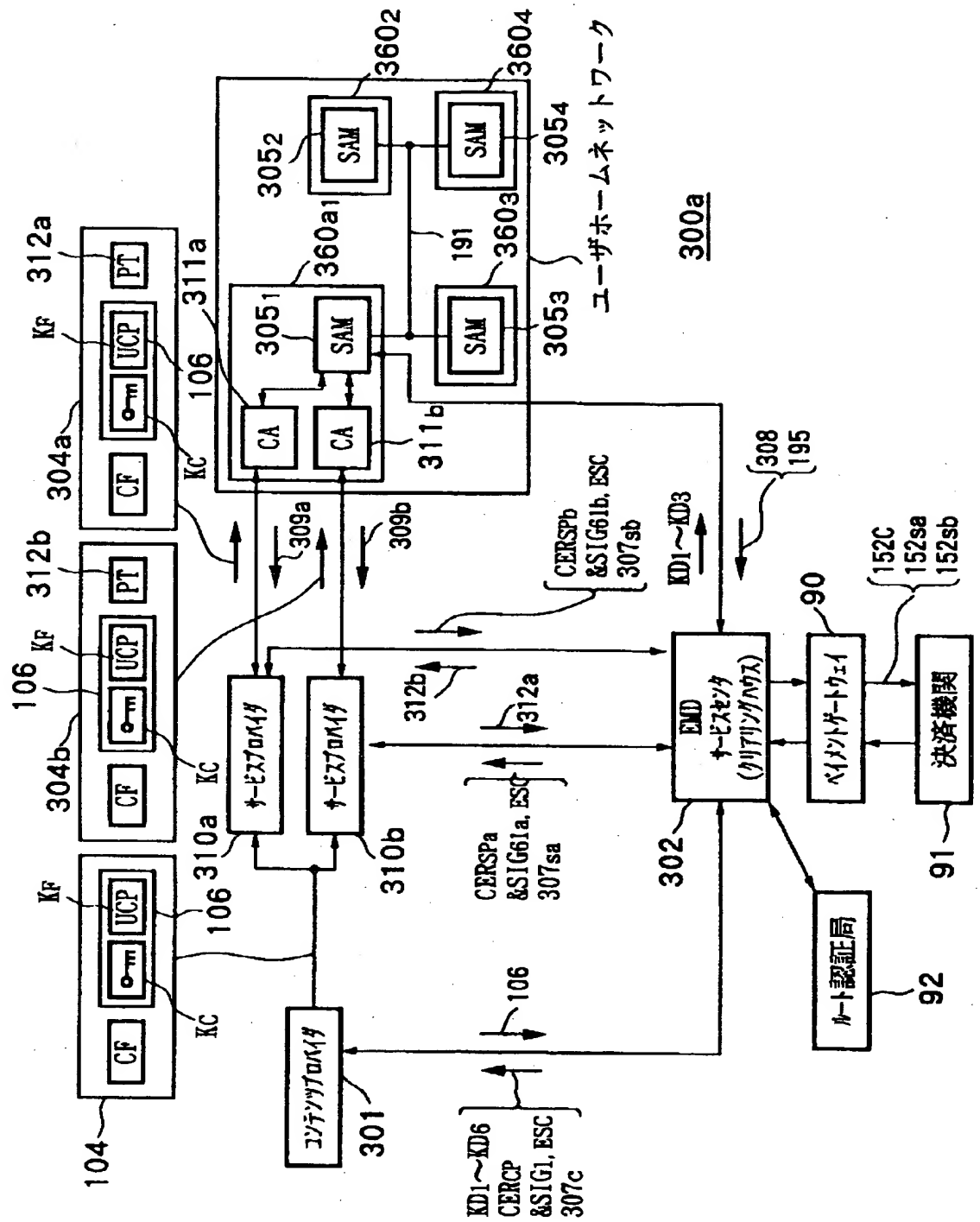
【図７８】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークに配信用鍵データを送信する
S21
EMDサービスセンタは権利書データを登録して権威化する
S22
コンテンツプロバイダからサービスプロバイダにセキュアコンテナに供給
S23
サービスプロバイダにおいて、セキュアコンテナの送信元の正当性を確認する
S24
サービスプロバイダにおいてプライスタグデータを作成し、セキュアコンテナ内にプライスタグデータを格納する
S25
EMDサービスセンタはプライスタグデータを登録して権威化する
S26
サービスプロバイダからCAモジュールにセキュアコンテナを供給
S27
CAモジュールにおいてSP用購入履歴データを作成し、サービスプロバイダに送信する
S28

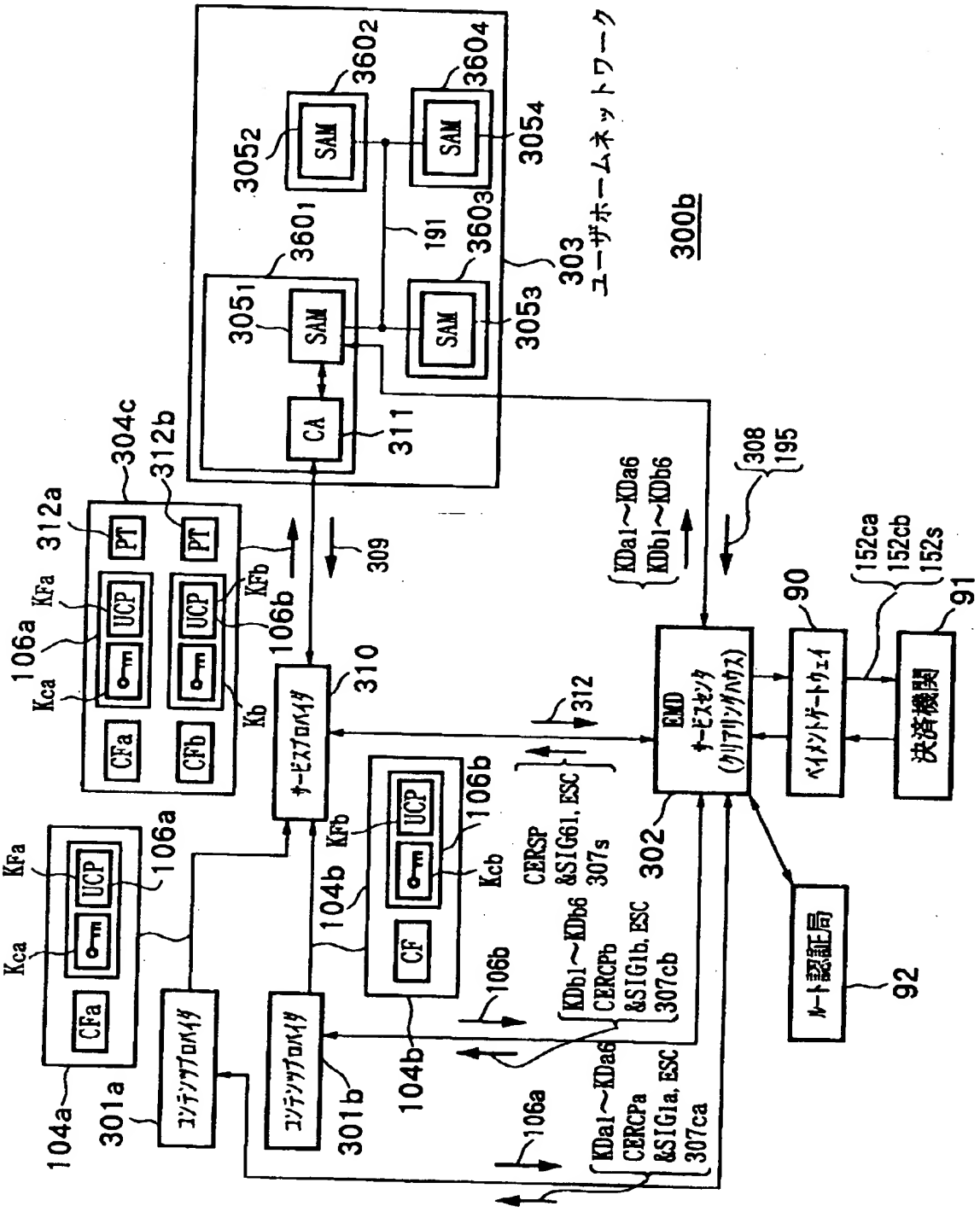
【図７９】


SAMにおいてサービスプロバイダの正当性を確認する
S29
SAMにおいてコンテンツプロバイダの正当性を確認する
S30
SAMを用いて、コンテンツデータの
購入・利用形態を決定する
S31
SAMにおいて利用履歴データを作成し、EMDサービスセンタ
に送信する
S32
EMDサービスセンタに行い、決済請求権データを作成する
S33
決済機関において、決済請求権データに基づいて
コンテンツプロバイダおよびサービスプロバイダに
利益が分配される
S34

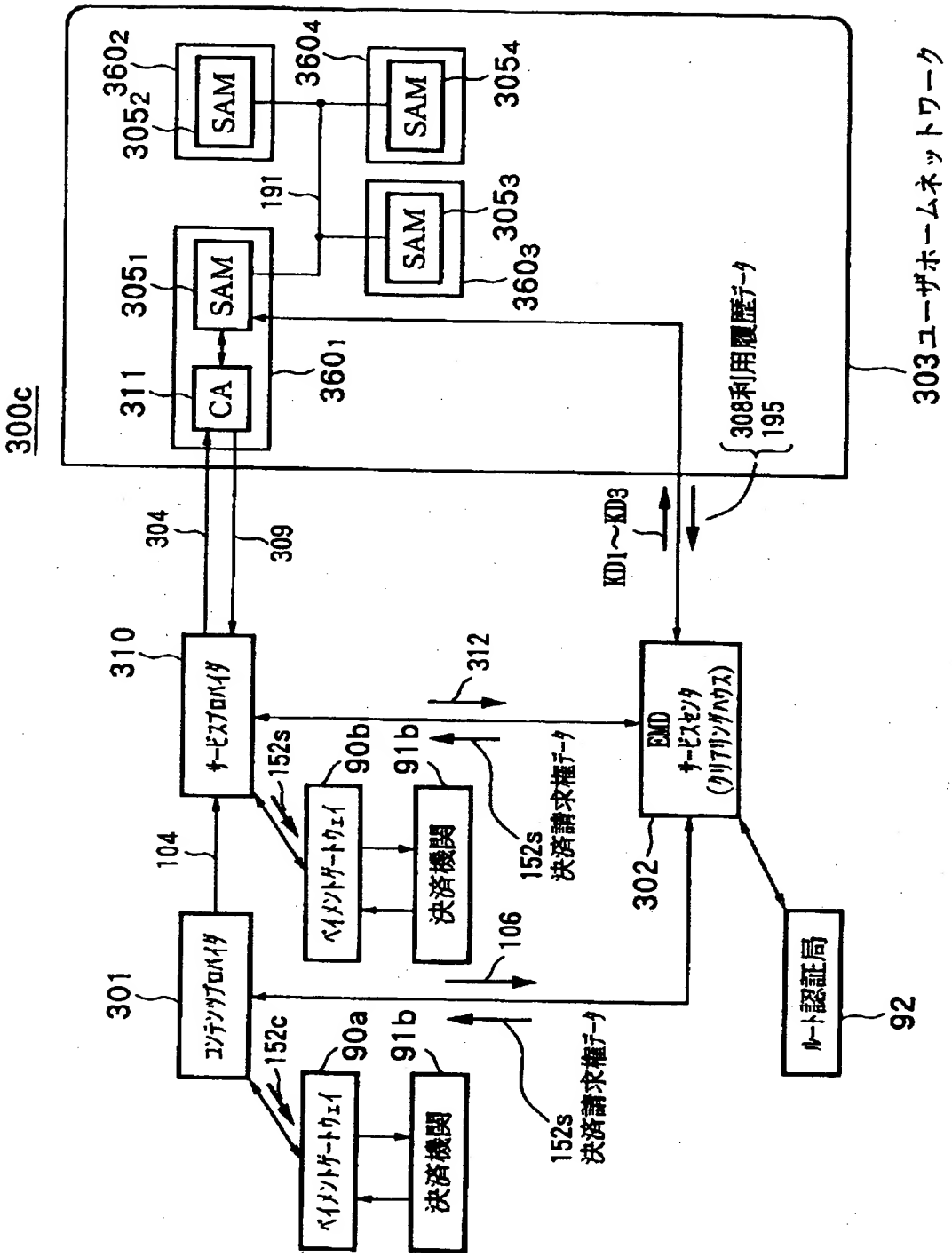
【図８０】


ユーザホームネットワーク
300a
SAM
CA
UCP
CF
PT
KF
KC
106
191
195
302
301
104
90
91
92
EMD
サービスセンタ
(クリアリングハウス)
ゲートウェイ
決済機関
ルート認証局
コンテンツプロバイダ
KD1～KD3
KD1～KD6
CERSPa
&SIG61a, ESC
307sa
CERSPb
&SIG61b, ESC
307sb
CERCP
&SIG1, ESC
307c
152C
152sa
152sb
308

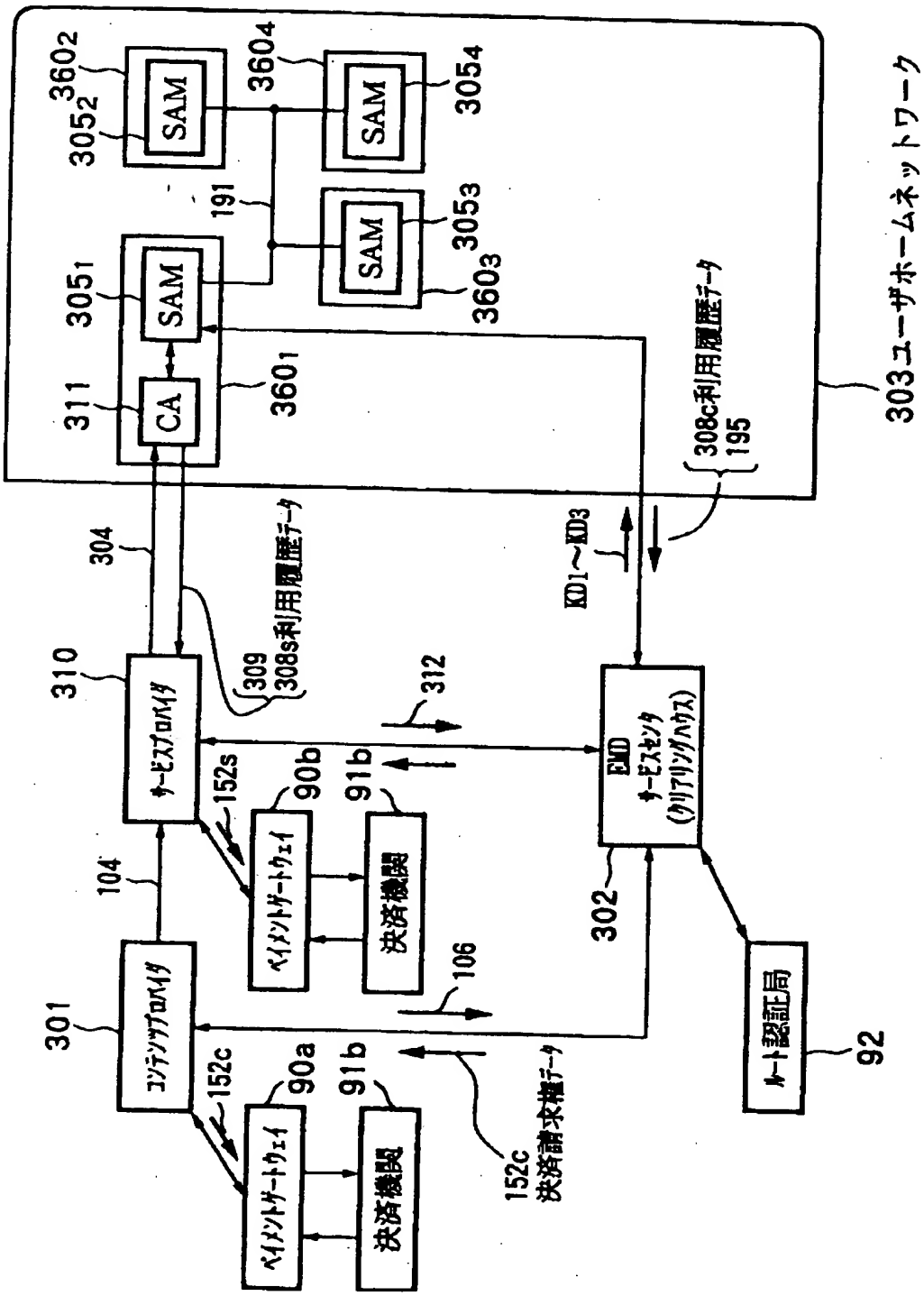
【図８１】


300b
303
ユーザホームネットワーク
SAM
CA
PT
UCP
CF
CFa
CFb
サービスプロバイダ
コンテンツプロバイダ
EMD
(クリアリングハウス)
ペイメントゲートウェイ
決済機関
ルート認証局
KDa1～KDa6
KDb1～KDb6
CERSP
&SIG61, ESC
307s
CERCPb
&SIG1b, ESC
307cb
CERCPa
&SIG1a, ESC
307ca

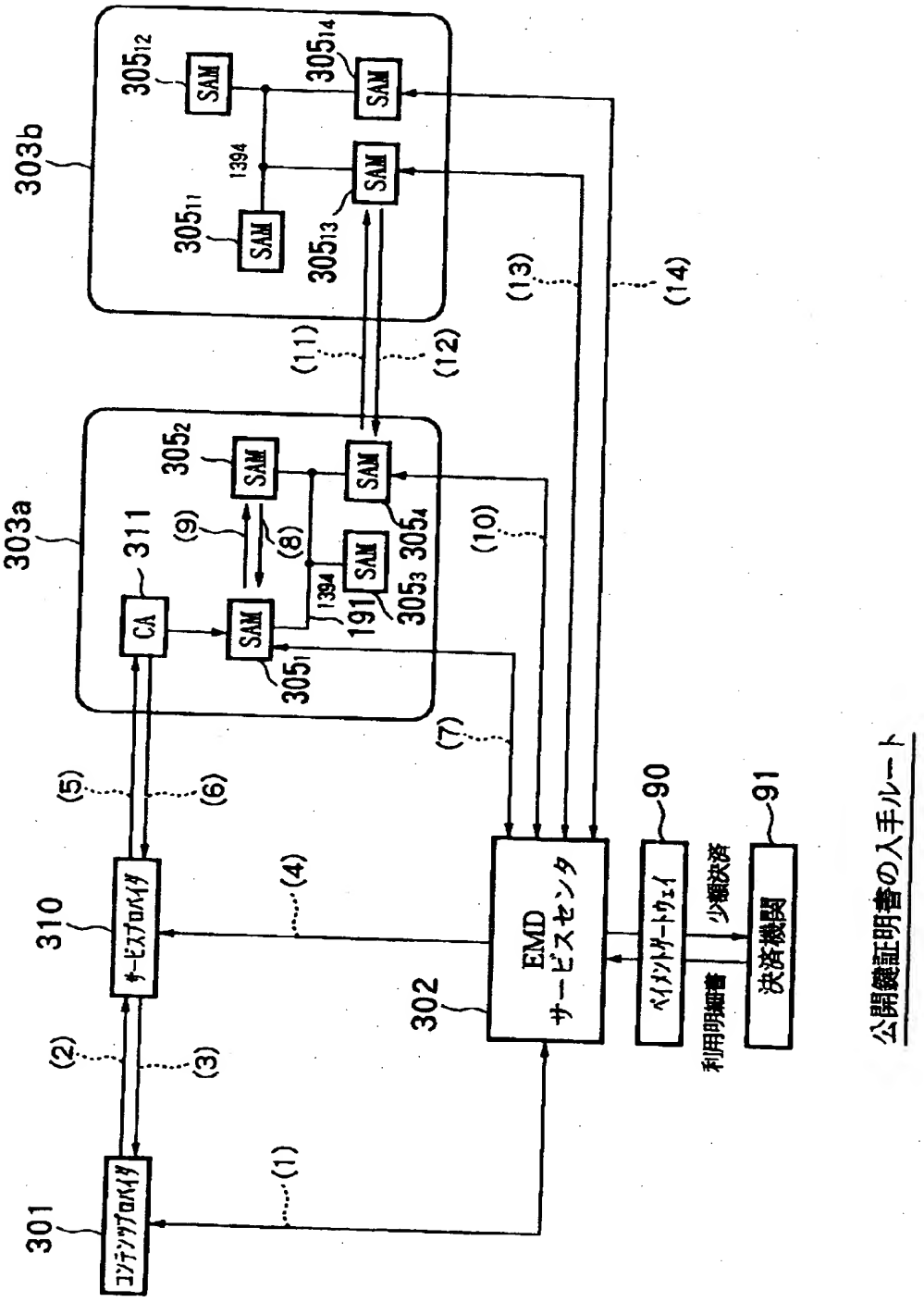
【図８２】


300c
303ユーザホームネットワーク
SAM
CA
311
304
309
310
サービスプロバイダ
312
152s
90b
91b
ペイメントゲートウェイ
決済機関
152s
決済請求権データ
104
301
コンテンツプロバイダ
152c
90a
91b
106
152s
決済請求権データ
KD1～KD3
308利用履歴データ
195
302
EMD
サービスセンタ
(クリアリングハウス)
ルート認証局
92

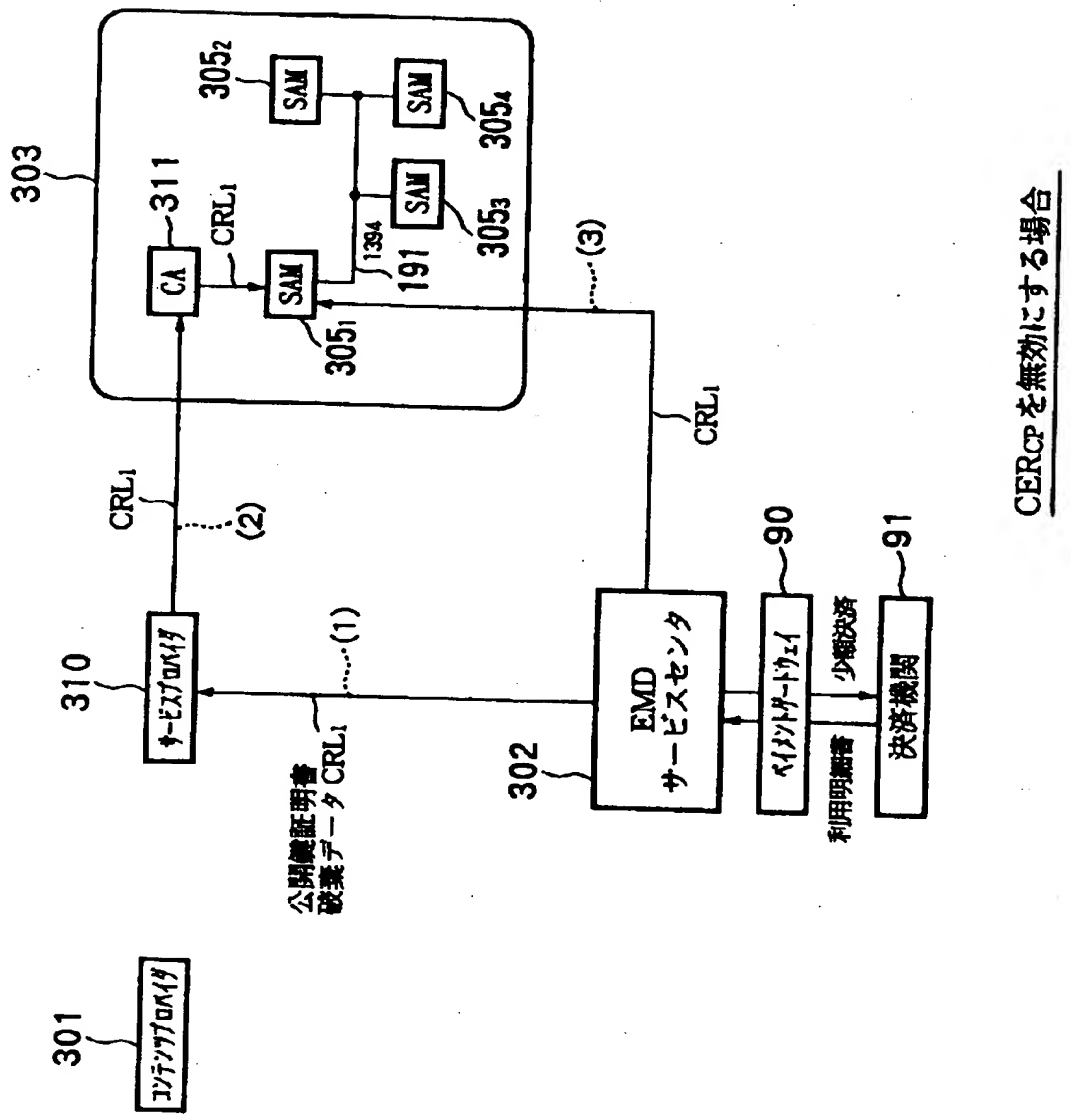
【図８３】


SAM
CA
303ユーザホームネットワーク
308c利用履歴データ
195
KD1～KD3
304
309
308s利用履歴データ
310
312
152s
90b
91b
104
106
302
152c
90a
91b
92
152c
決済請求権データ
決済機関
ルート認証局

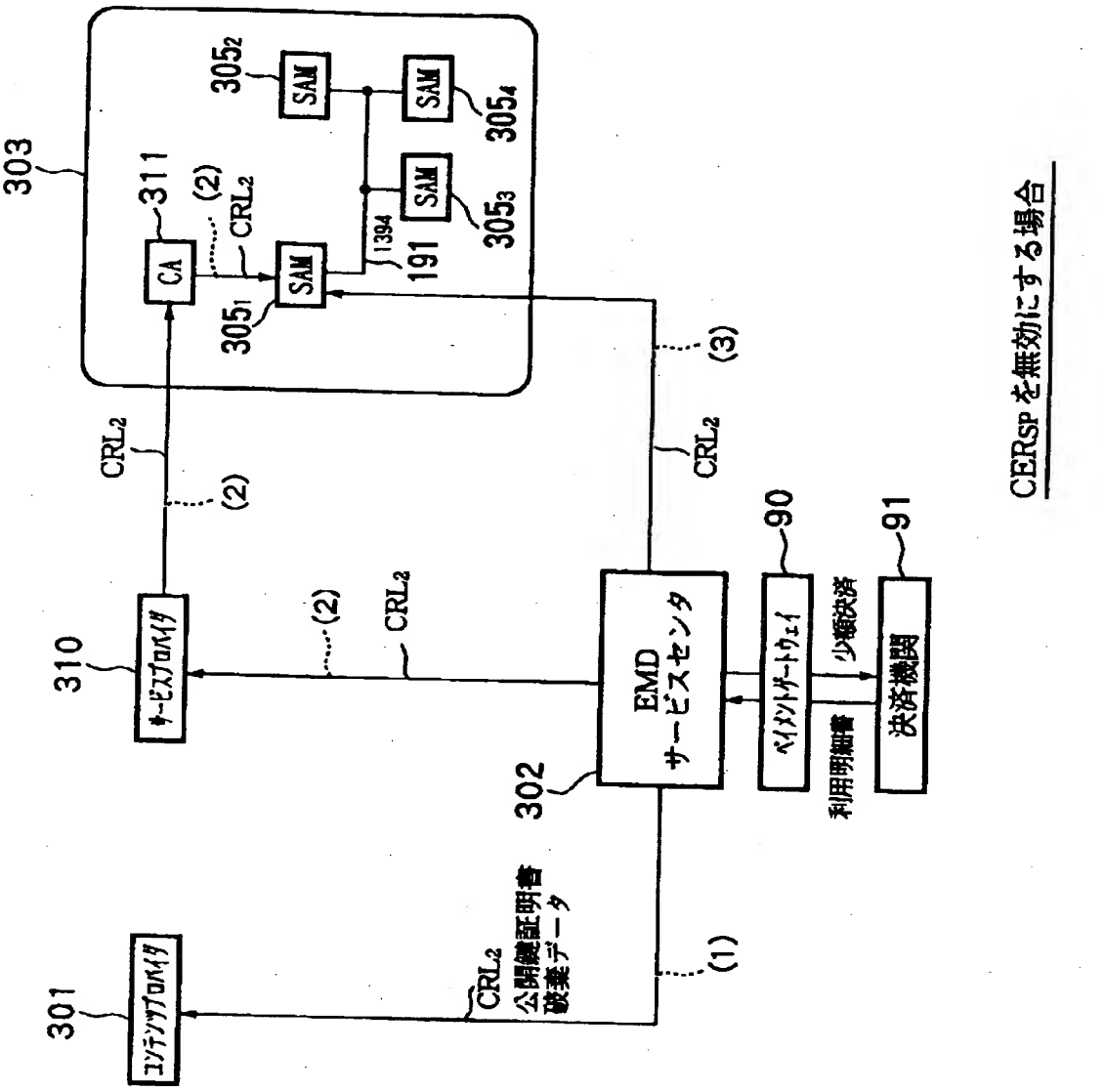
【図８４】


303b
305_{12}
305_{14}
305_{11}
305_{13}
SAM
1394
303a
311
305_2
305_4
305_3
305_1
CA
191
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)
301
コンテンツプロバイダ
310
サービスプロバイダ
302
EMD
サービスセンタ
90
ペイメントゲートウェイ
91
決済機関
少額決済
利用明細書
公開鍵証明書の入手ルート

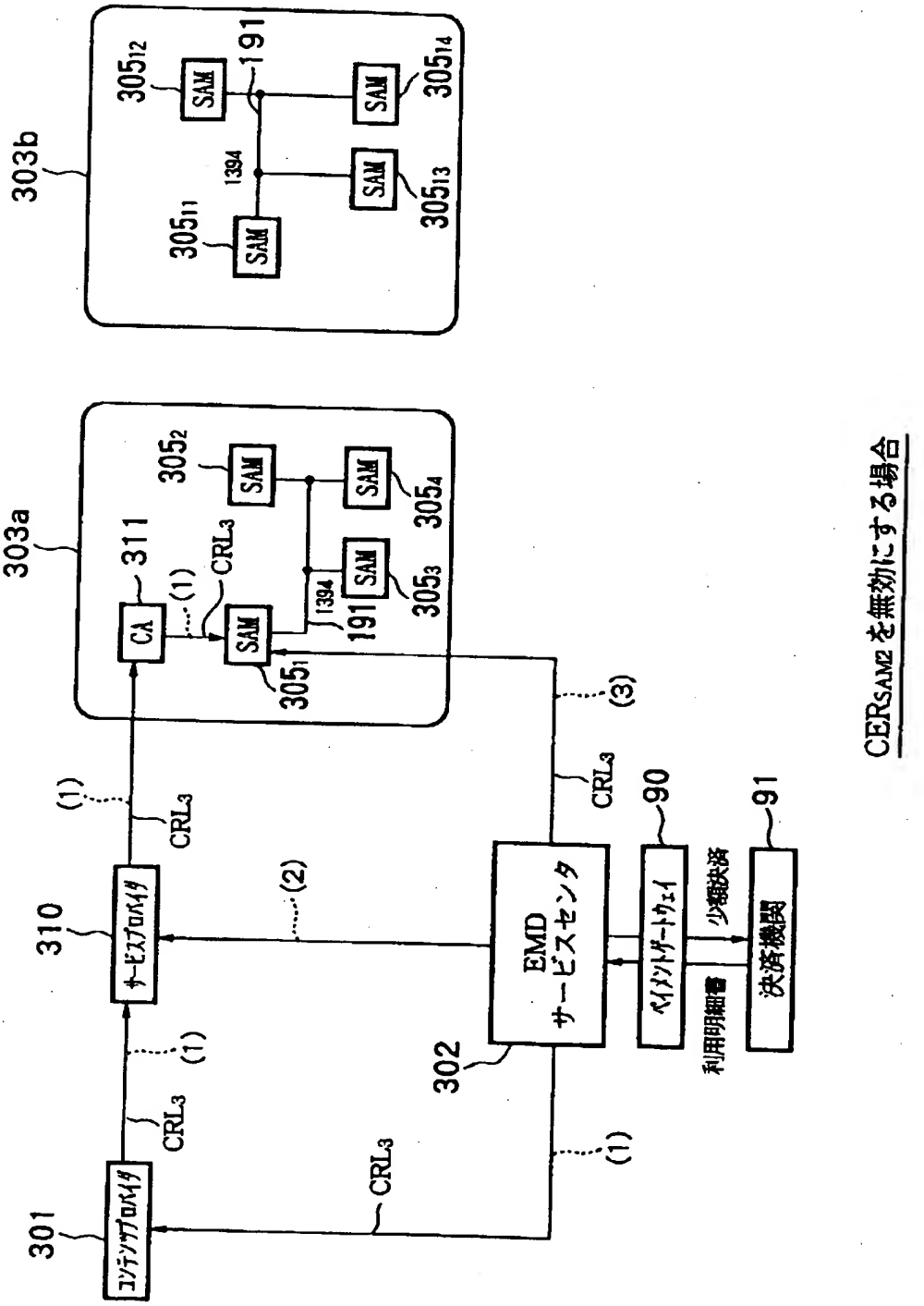
【図８５】


303
311
CA
CRL1
SAM
3052
SAM
3054
SAM
3053
1394
191
3051
(3)
CRL1
CRL1
(2)
310
サービスプロバイダ
(1)
公開鍵証明書
秘密データ CRL1
302
EMD
サービスセンタ
90
ペイメントゲートウェイ
少額決済
利用明細書
91
決済機関
301
コンテンツプロバイダ
CERCP を無効にする場合

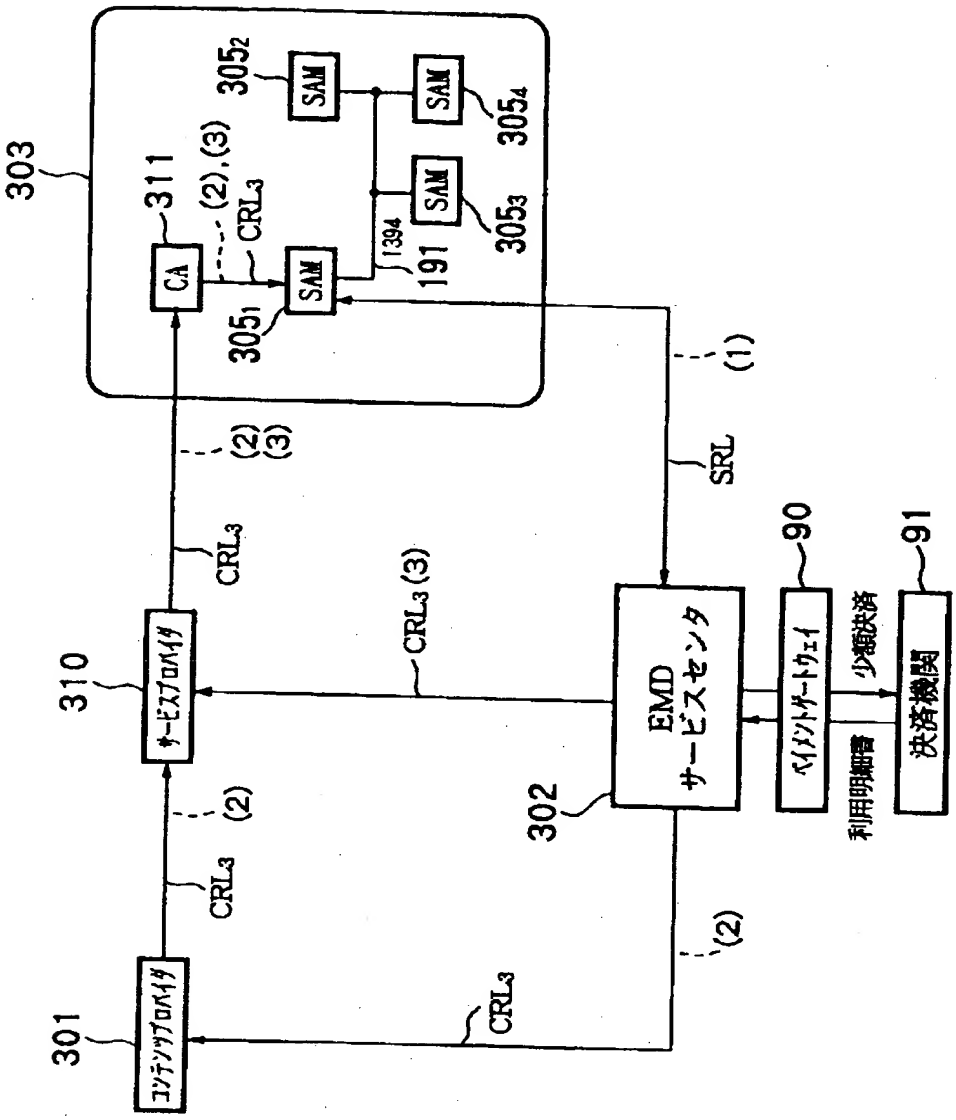
【図８６】


303
311
CA
(2)
CRL2
SAM
3051
3052
3053
3054
1394
191
(3)
CRL2
(2)
CRL2
310
サービスプロバイダ
(2)
CRL2
EMD
サービスセンタ
302
90
ペイメントゲートウェイ
少額決済
利用明細書
91
決済機関
CRL2
公開鍵証明書
破棄データ
(1)
301
エンティティプロバイダ
CERSPを無効にする場合

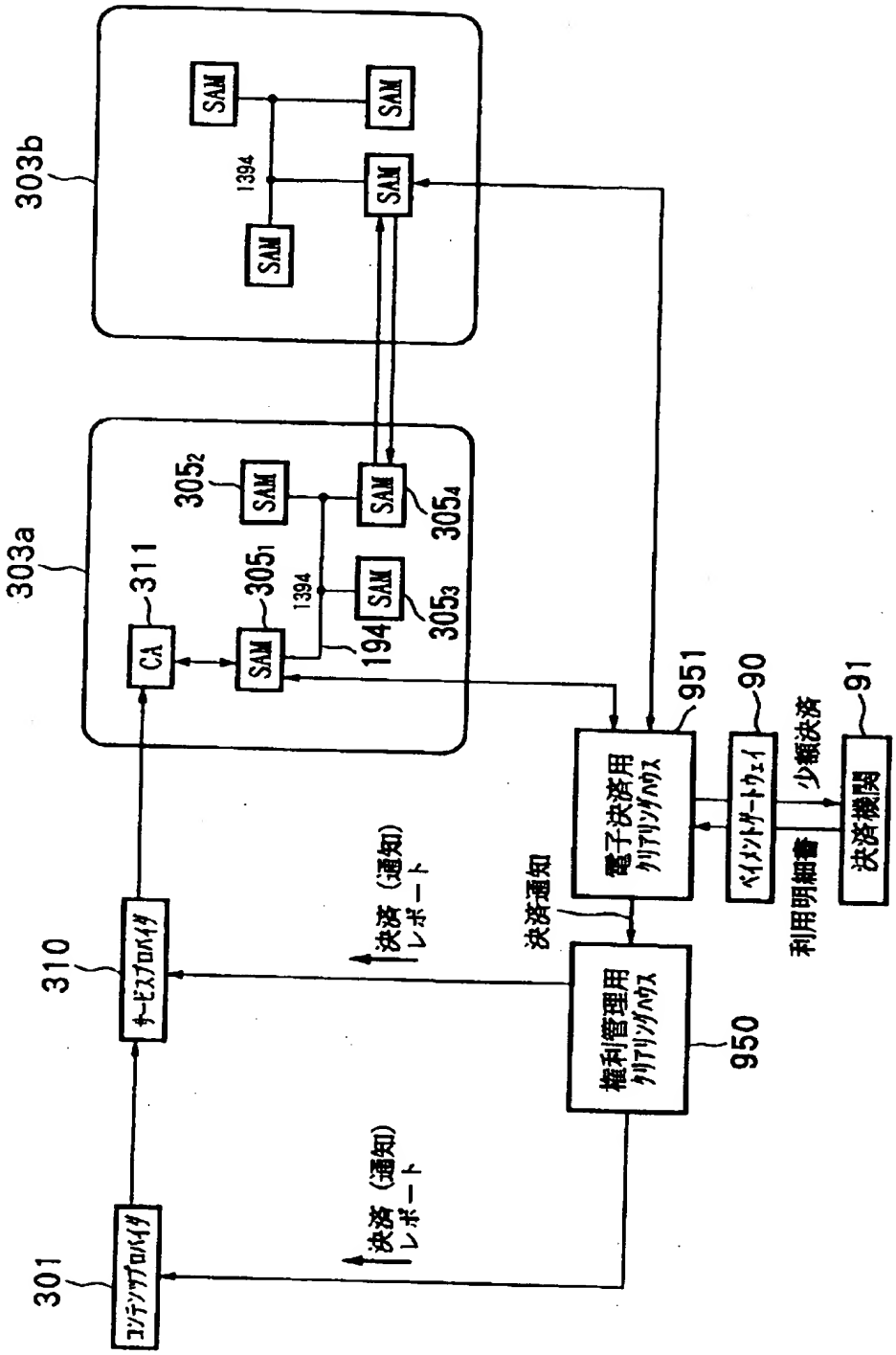
【図８７】


303b
305₁₂
SAM
191
305₁₄
SAM
1394
SAM
305₁₃
305₁₁
SAM
303a
311
305₂
SAM
SAM
305₄
CA
(1)
CRL₃
1394
SAM
191
305₃
SAM
305₁
(3)
CRL₃
(1)
CRL₃
310
サービスプロバイダ
(2)
EMD
サービスセンタ
90
91
ペイメントゲートウェイ
少額決済
利用明細書
決済機関
(1)
CRL₃
302
(1)
CRL₃
301
コンテンツプロバイダ
CERSAM2を無効にする場合

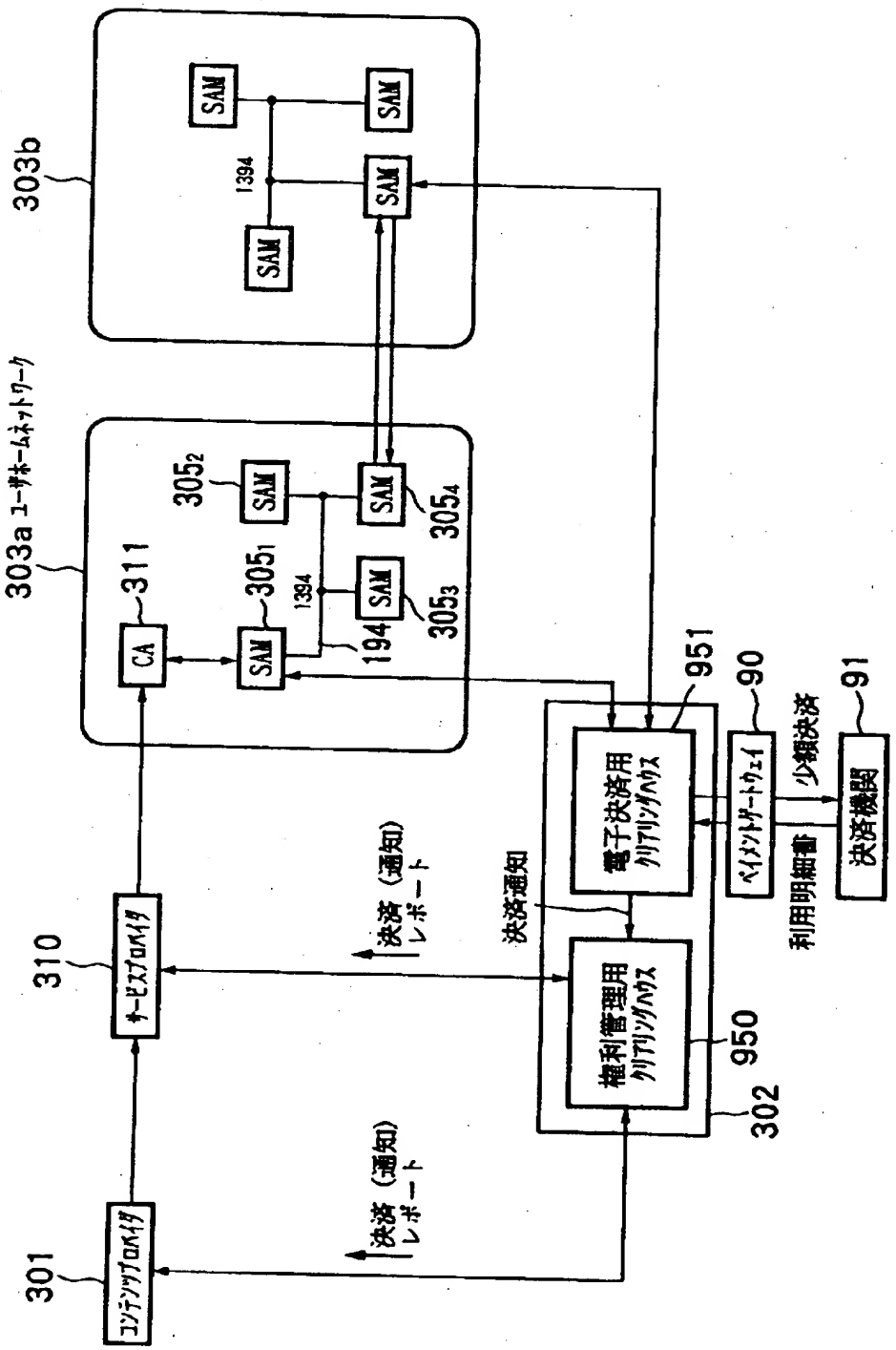
【図８８】


303
311
CA
SAM
305_1
305_2
305_3
305_4
1394
191
(2),(3)
CRL_3
(1)
SRL
(2)
(3)
310
サービスプロバイダ
EMD
サービスセンタ
302
90
ペイメントゲートウェイ
91
決済機関
少額決済
利用明細書
(2)
301
コンテンツプロバイダ

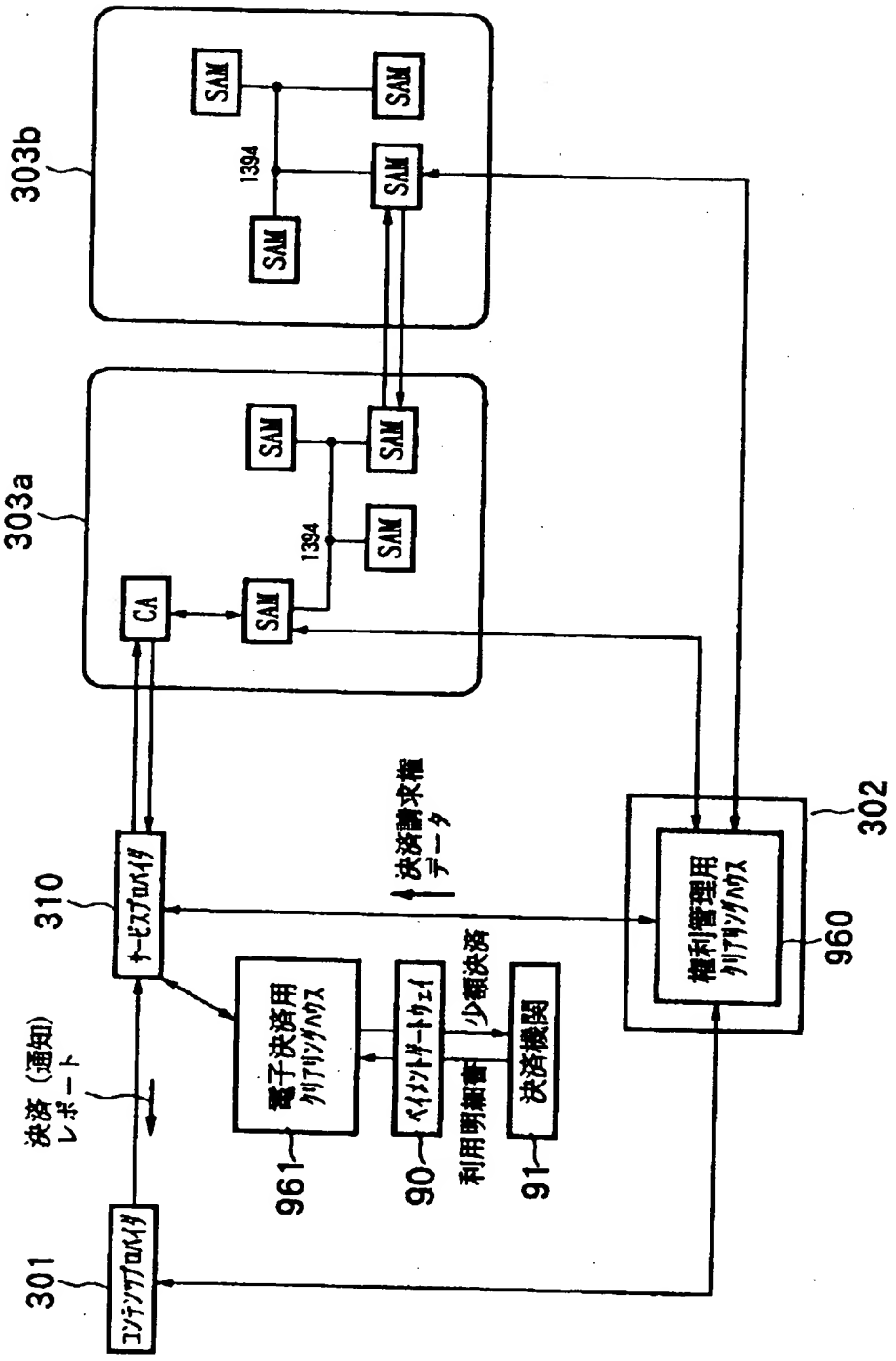
【図８９】


303b
SAM
SAM
1394
SAM
SAM
303a
305_2
SAM
SAM
305_4
311
CA
305_1
SAM
1394
SAM
305_3
194
951
電子決済用クリアリングハウス
90
ペイメントゲートウェイ
91
決済機関
少額決済
利用明細書
決済通知
決済（通知）レポート
310
サービスプロバイダ
権利管理用クリアリングハウス
950
決済（通知）レポート
301
コンテンツプロバイダ

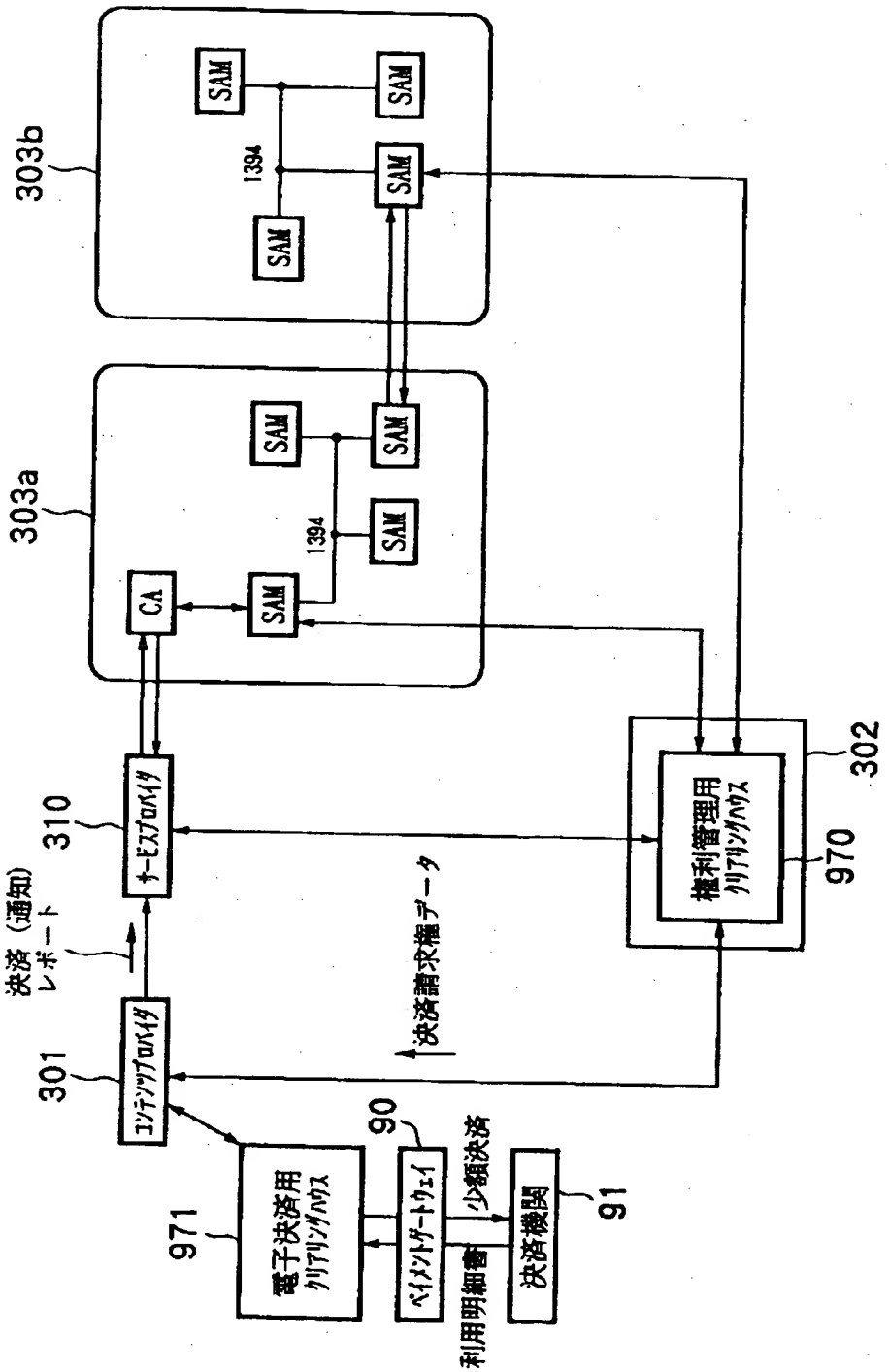
【図９０】


303b
SAM
1394
303a ユーザホームネットワーク
305₂
305₄
305₁
305₃
311
CA
194
310
サービスプロバイダ
301
コンテンツプロバイダ
決済（通知）レポート
決済通知
電子決済用クリアリングハウス
951
権利管理用クリアリングハウス
950
302
ペイメントゲートウェイ
90
少額決済
利用明細書
決済機関
91

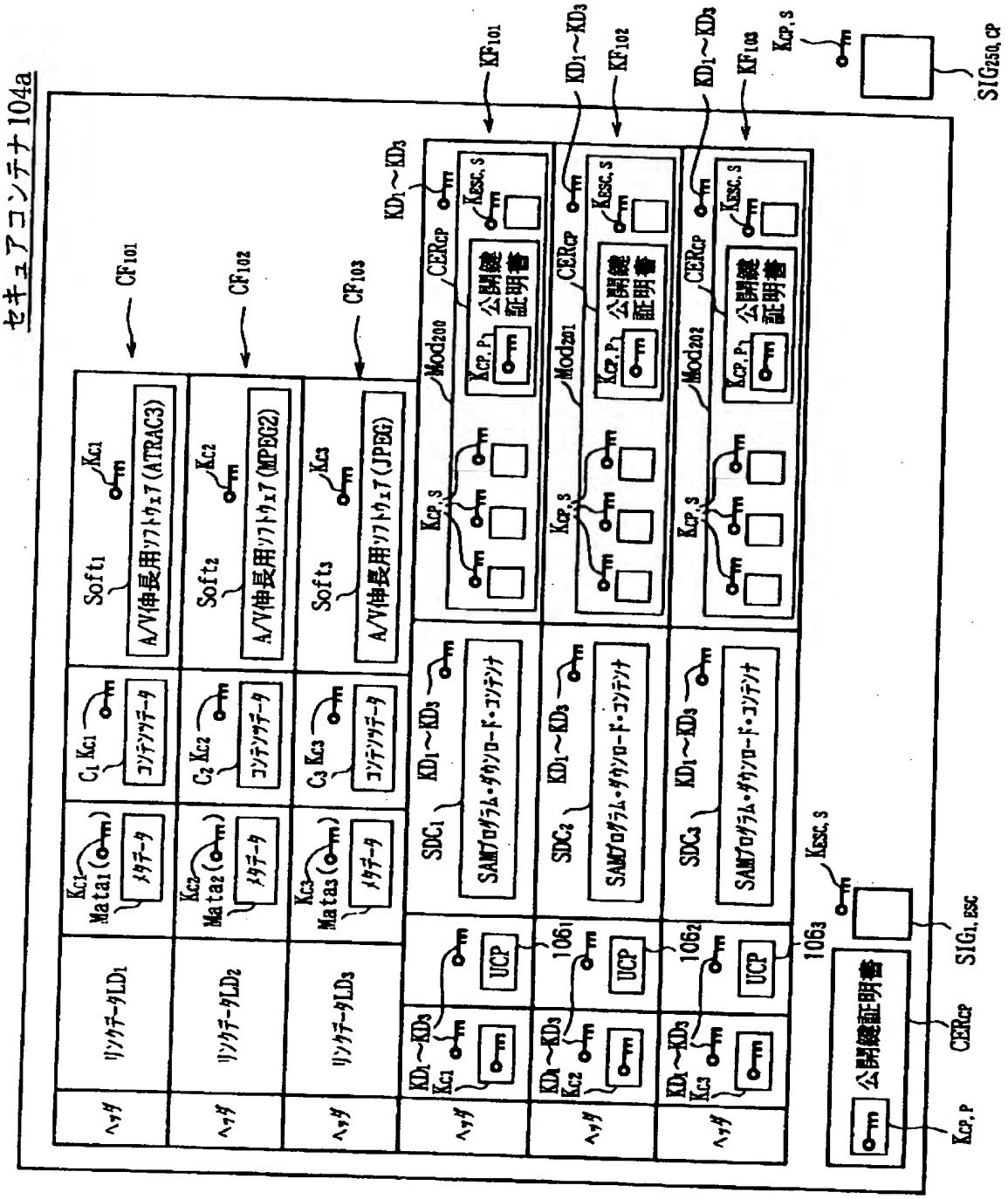
【図９１】


303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
決済請求権
データ
310
302
960
権利管理用
クリアリングハウス
サービスプロバイダ
電子決済用
クリアリングハウス
ペイメントゲートウェイ
少額決済
利用明細書
決済機関
決済（通知）
レポート
961
90
91
301
コンテンツプロバイダ

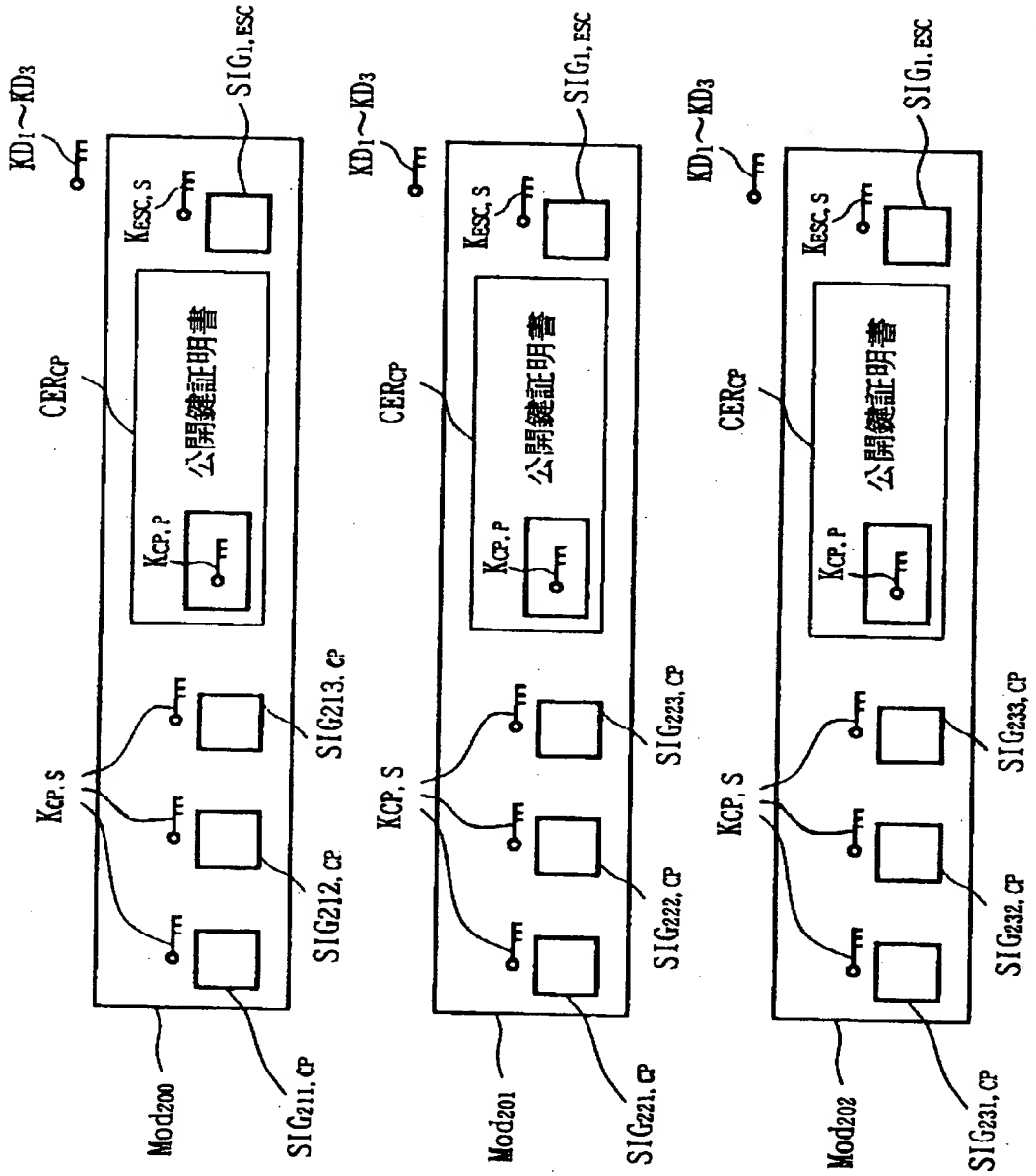
【図９２】


303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
310
サービスプロバイダ
302
権利管理用
クリアリングハウス
970
決済（通知）
レポート
決済請求権データ
301
コンテンツプロバイダ
90
971
電子決済用
クリアリングハウス
ペイメントゲートウェイ
少額決済
利用明細書
決済機関
91

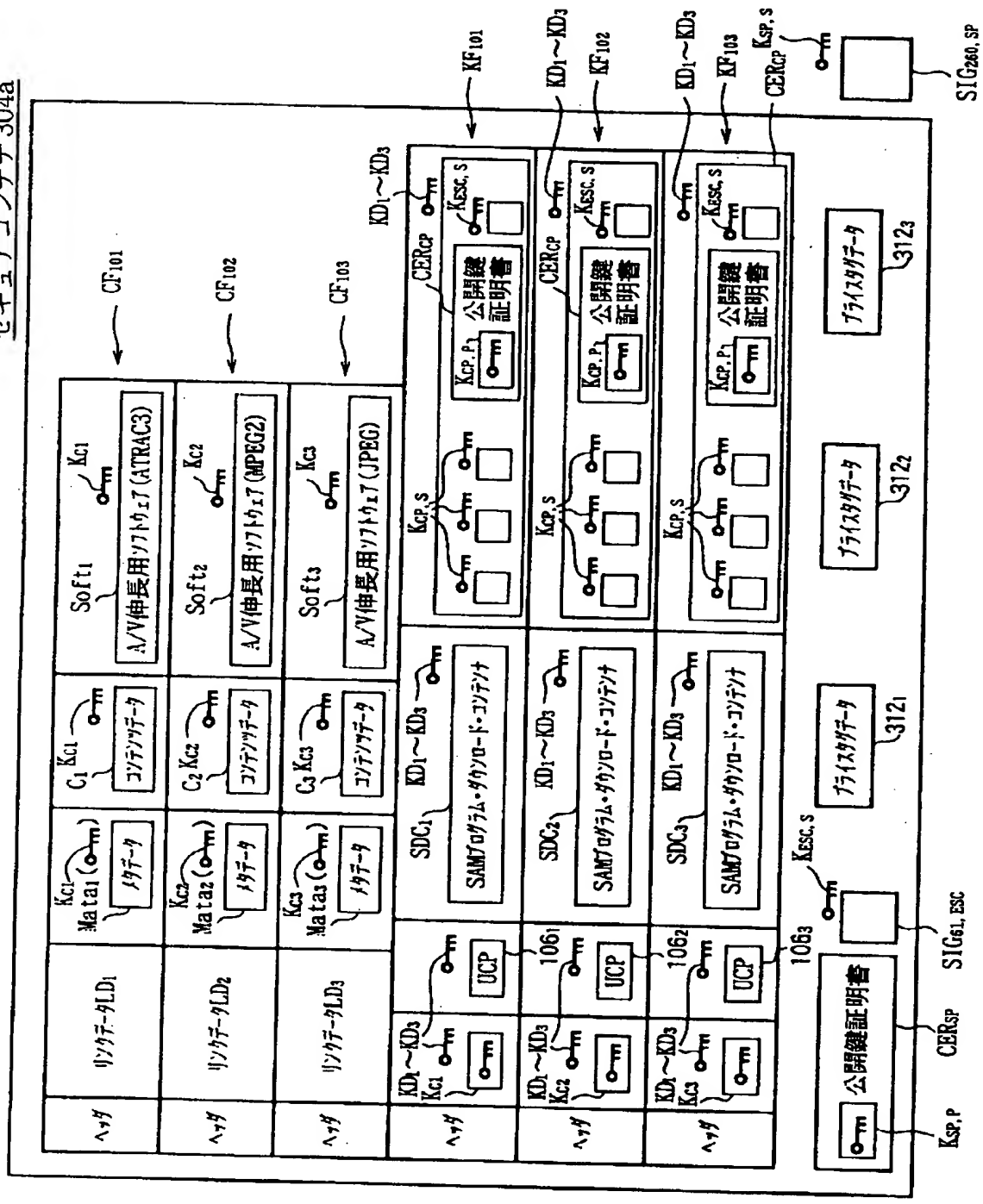
【図９３】


セキュアコンテナ104a
ヘッダ
リンクデータLD1
リンクデータLD2
リンクデータLD3
Kc1 Mata1
Kc2 Mata2
Kc3 Mata3
メタデータ
C1 Kc1
C2 Kc2
C3 Kc3
コンテンツデータ
Soft1
Soft2
Soft3
Kc1
Kc2
Kc3
A/V伸長用ソフトウェア(ATRAC3)
A/V伸長用ソフトウェア(MPEG2)
A/V伸長用ソフトウェア(JPEG)
CF101
CF102
CF103
KD1～KD3
KF101
KF102
KF103
Mod200
Mod201
Mod202
CERCP
KCP,S
KESC,S
KCP,P1
公開鍵証明書
SDC1
SDC2
SDC3
KD1～KD3
SAMプログラム・ダウンロード・コンテンツ
UCP
1061
1062
1063
KESC,S
KCP,P
公開鍵証明書
CERCP
SIG1,ESC
KCP,S
SIG250,CP

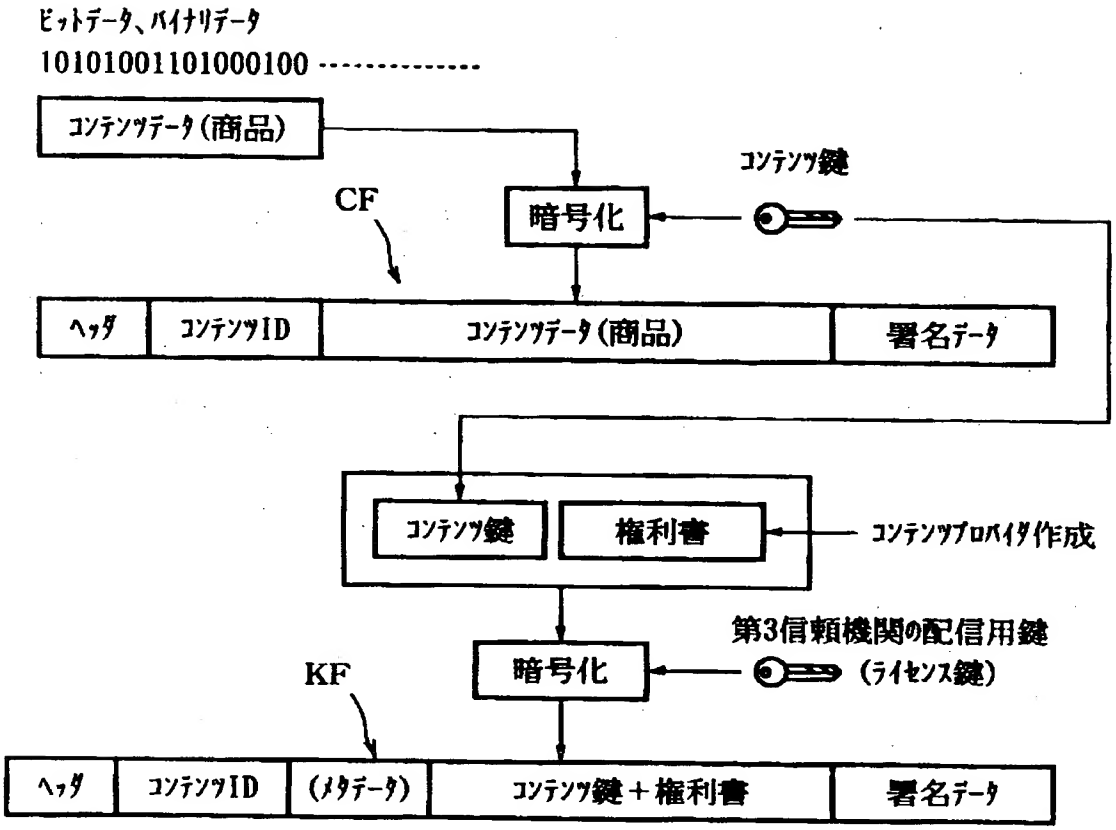
【図９４】


KD1～KD3
SIG1, ESC
KESC, S
CERCP
公開鍵証明書
KCP, P
KCP, S
SIG213, CP
SIG212, CP
SIG211, CP
Mod200
SIG223, CP
SIG222, CP
SIG221, CP
Mod201
SIG233, CP
SIG232, CP
SIG231, CP
Mod202

【図９５】

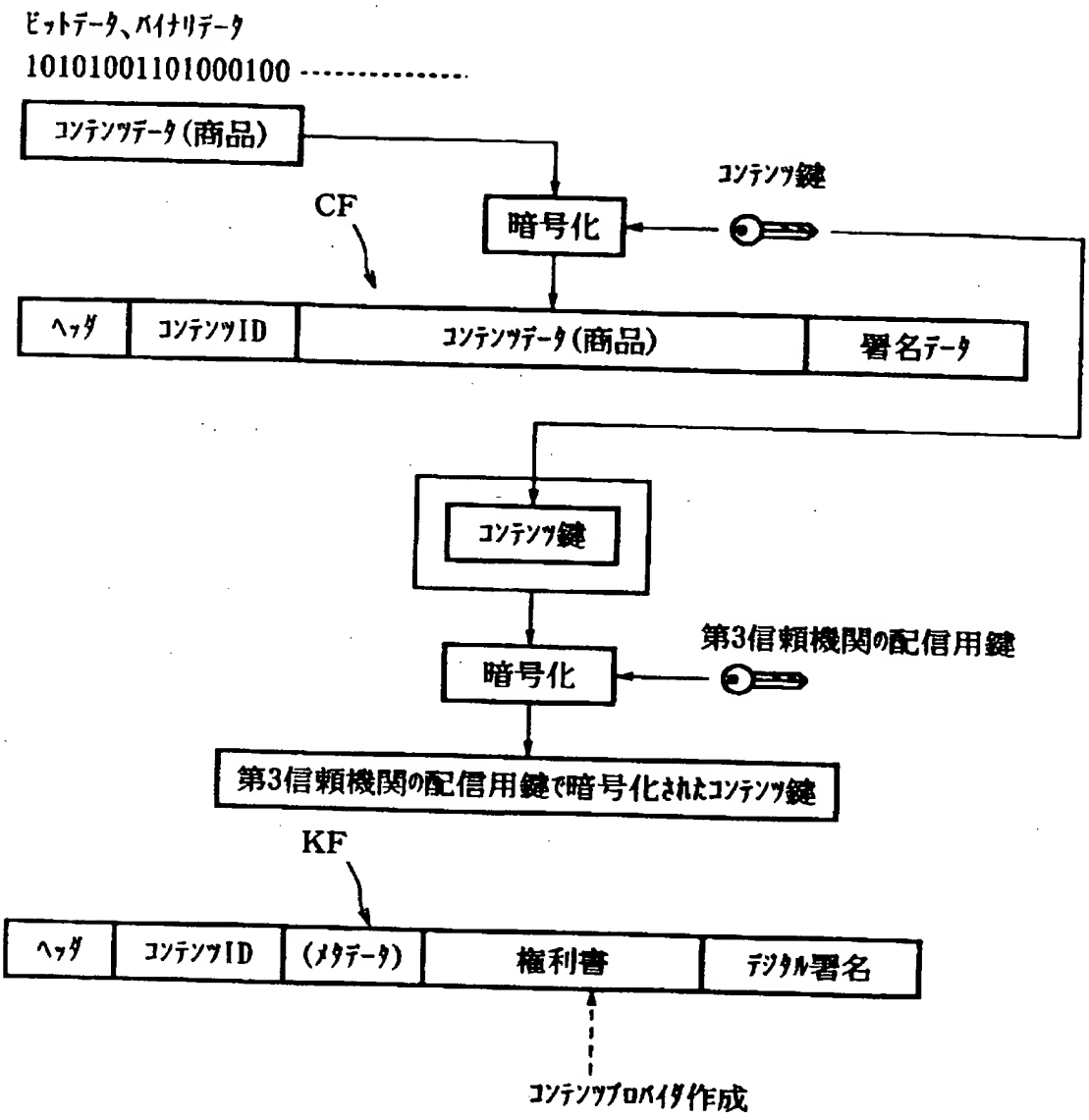

セキュアコンテナ304a
ヘッダ
リンクデータLD1
リンクデータLD2
リンクデータLD3
Kc1 Meta1 メタデータ
Kc2 Meta2 メタデータ
Kc3 Meta3 メタデータ
C1 Kc1 コンテンツデータ
C2 Kc2 コンテンツデータ
C3 Kc3 コンテンツデータ
Soft1 Kc1 A/V伸長用ソフトウェア(ATRAC3)
Soft2 Kc2 A/V伸長用ソフトウェア(MPEG2)
Soft3 Kc3 A/V伸長用ソフトウェア(JPEG)
CF101
CF102
CF103
KD1～KD3
SDC1
SDC2
SDC3
SAMプログラム・ダウンロード・コンテンツ
UCP
1061
1062
1063
KCP, S
KCP, P1
CERCP
公開鍵証明書
KESC, S
KF101
KF102
KF103
KD1～KD3
CERCP
KSP, S
SIG260, SP
プライスタグデータ
3121
3122
3123
KSP, P
CERSP
KESC, S
SIG61, ESC

【図９６】



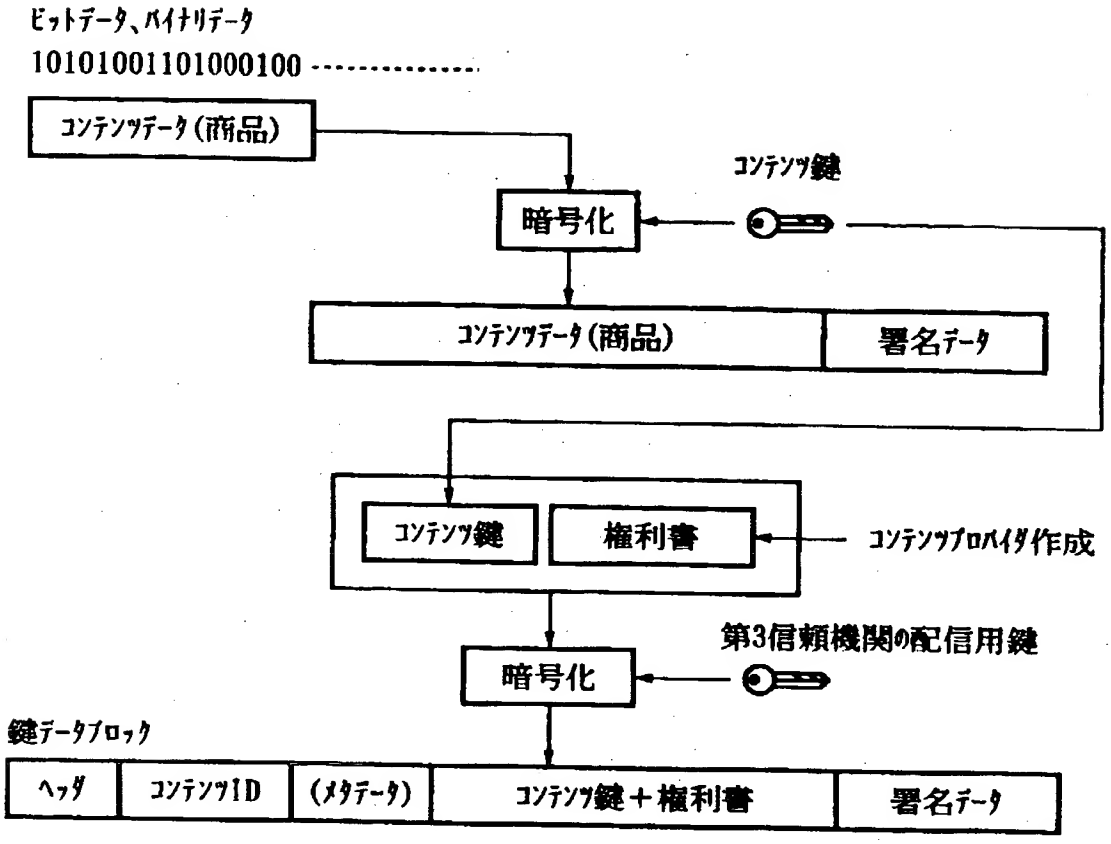
インターネット(その1)

【図９７】



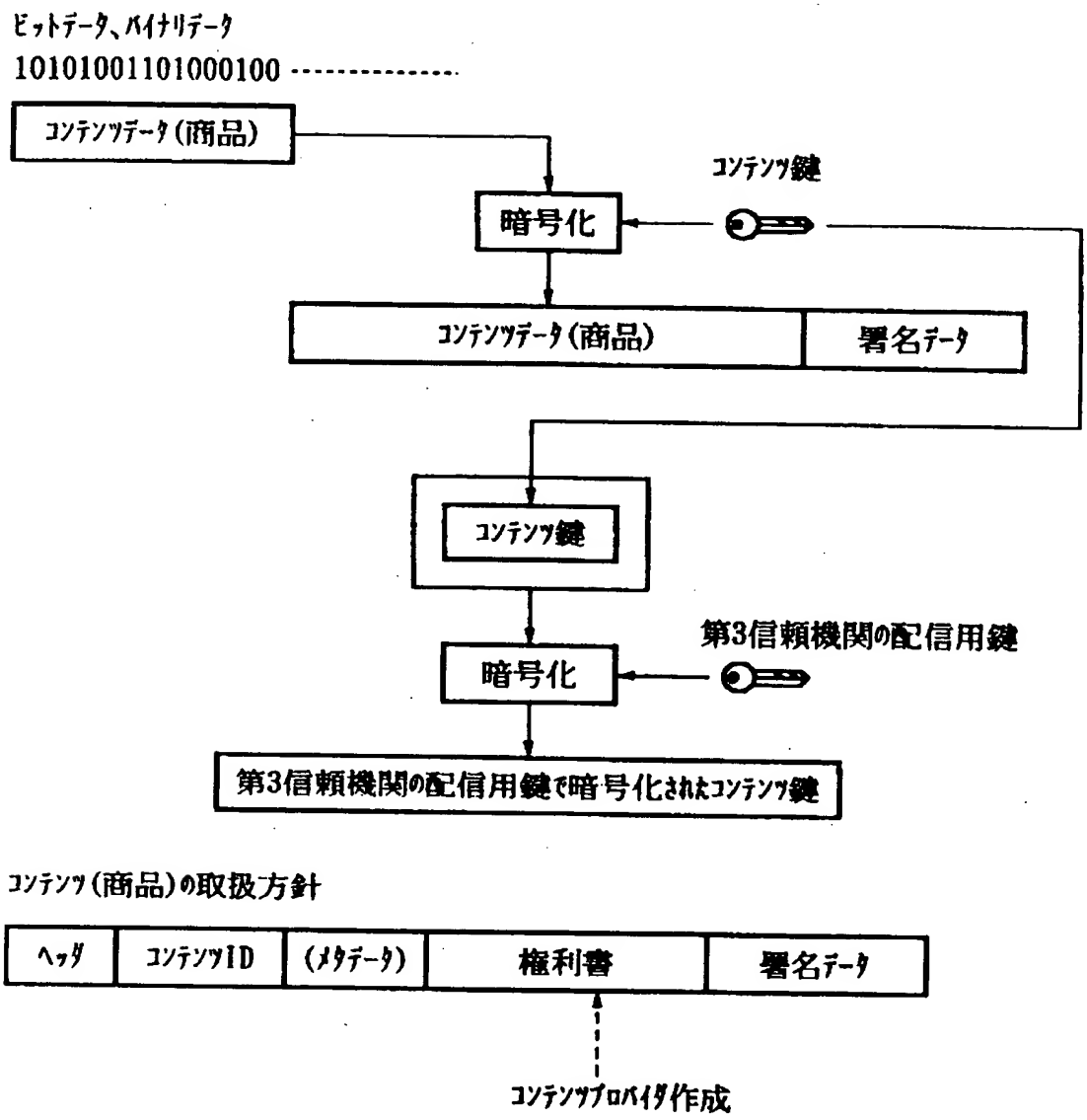
インターネット(その2)

【図９８】



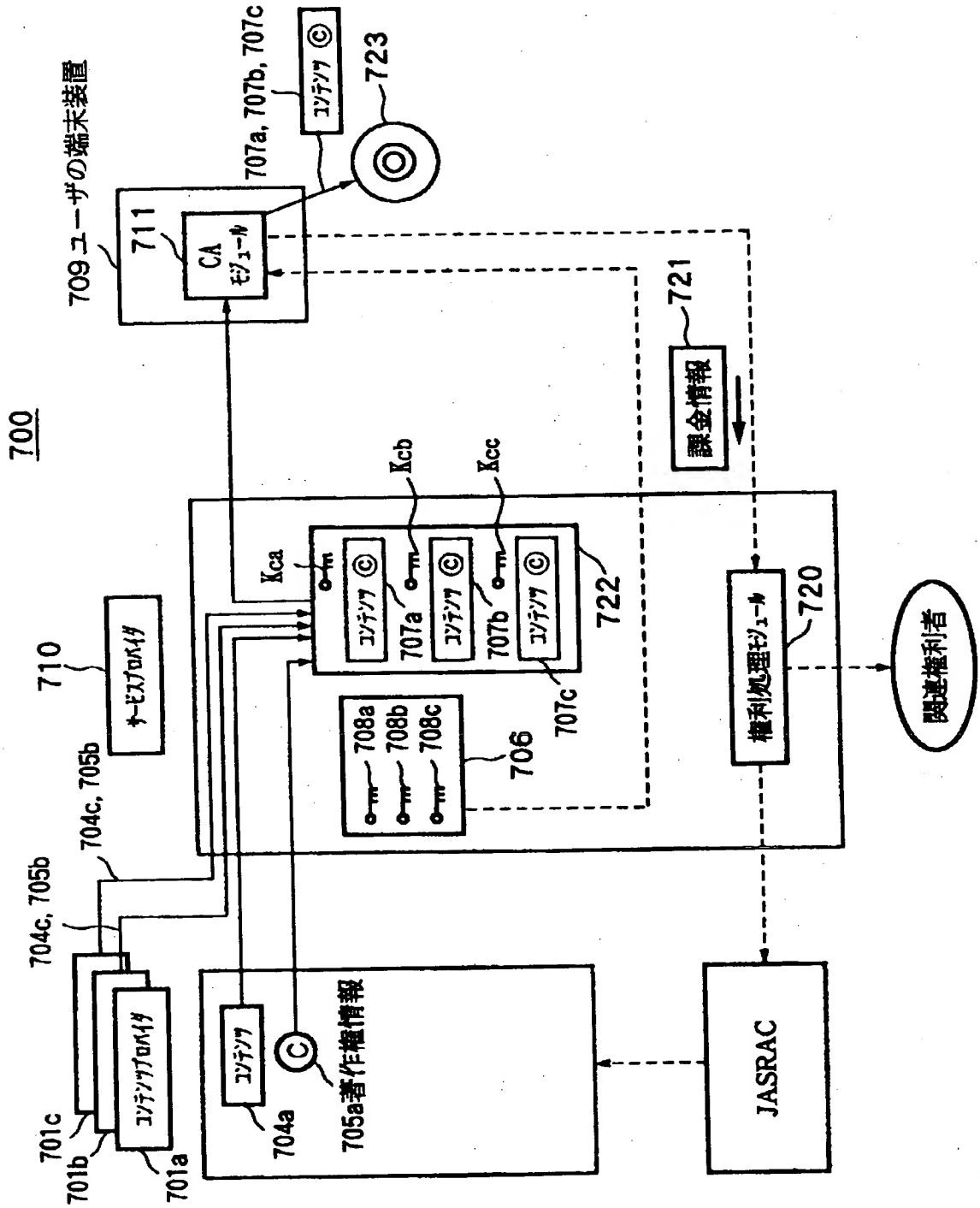
デジタル放送(その1)

【図９９】



デジタル放送(その2)

【図１００】


700
709 ユーザの端末装置
711
CA モジュール
707a, 707b, 707c
コンテンツ ©
723
721
課金情報
710
サービスプロバイダ
Kca
Kcb
Kcc
コンテンツ ©
707a
707b
707c
722
708a
708b
708c
706
権利処理モジュール
720
関連権利者
704c, 705b
704c, 705b
コンテンツプロバイダ
701c
701b
701a
コンテンツ
704a
© 705a著作権情報
JASRAC

【書類名】　　要約書

【要約】

【課題】　データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。

【解決手段】　コンテンツプロバイダ１０１は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、配信鍵用データを用いて暗号化されたコンテンツ鍵データと、コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したセキュアコンテナ１０４をユーザホームネットワーク１０３のＳＡＭ105_1などに配給する。ＳＡＭ105_1などは、セキュアコンテナ１０４に格納されたコンテンツ鍵データおよび権利書データを復号し、当該復号した権利書データに基づいて、コンテンツデータの購入形態および利用形態などの取り扱いを決定する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－１２６３０５
受付番号	５００００５０２８７８５
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１２年　４月２６日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川６丁目７番３５号
【氏名又は名称】	ソニー株式会社

【代理人】　申請人

【識別番号】	100094053
【住所又は居所】	東京都台東区柳橋２丁目４番２号　創進国際特許事務所
【氏名又は名称】	佐藤　隆久

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社